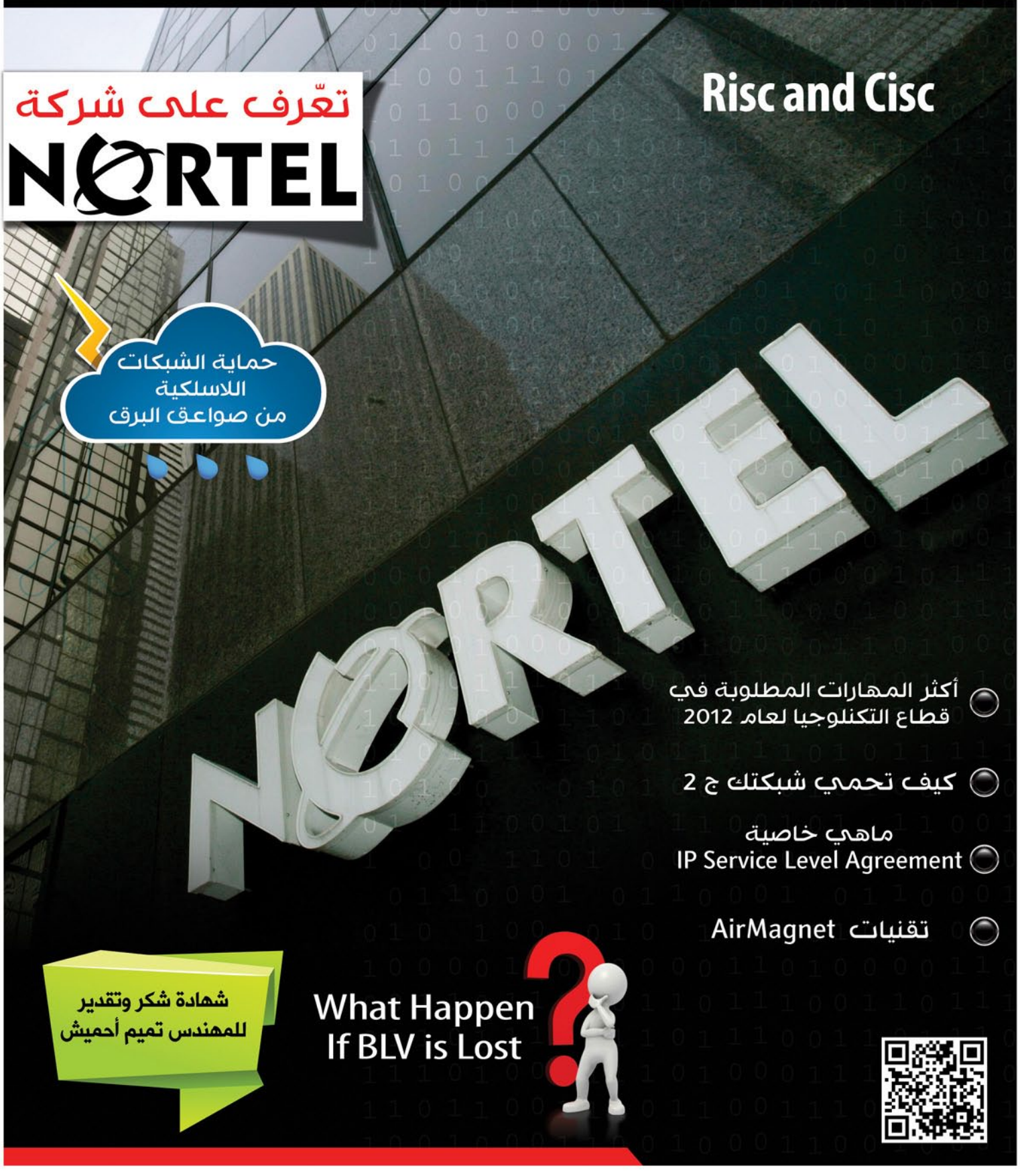
NO. 22 January 2012 • Price Free • www.networkset.net

NetWork Set

First Arabic Magazine For Networks



تجربتي مع تنظيم الوقت

عندما كنا صغارا كان أهلنا ينصحونا دائما بتنظيم أوقاتنا وأذكر أن عندما كنت أدرس في المرحلة الإعدادية وتحديدا في الصف التاسع كنا نقوم بعمل جداول للوقت ونحدد فيه وقت المدرسة أكلنا ونومنا وماذا ندرس ومتى نرتاح وحتى متى وكم نشاهد التلفاز وكل التفاصيل التى أحتاجها لتنظيم وقتي ولكن المشكلة التى أذكرها أيضا أن لم أتقيد ولامرة بهذا الجدول لأكثر من يومين وبعدها يزول كل شيئ ويعود إلى ماهو عليه وكأن شيئ لم يكن وتسوء الأمور مع الوقت ويبدأ التقصير وأعتقد أن أغلبكم مرة بتجارب مثل هذه .

هذه التجارب الفاشلة لم تكن تنجح ولن تنجح لأن تقييد الشخص بهذه الطريقة مستحيل لأن طارئ واحد يحدث معك في اليوم قد يسبب لك تغيير الجدول وبالتالي تقل الثقة في الجدول المخصص , لذلك لنسأل أنفسنا مرة آخرى كيف ننظم وقتنا ونستغله ؟.

قبل أن أدخل بالطريقة والكيفية لنوضح اسباب إضاعة الوقت , أعتبر السبب الأول والآخير في مسألة إضاعة الوقت هو في تحديد المهام فعندما نبدأ يومنا ونحن لانملك أي مهام يتوجب علينا إنجازها فهذا يعني أن اليوم قد ضاع منك ليس فقط لأنك لاتملك المهام بل لأنك سوف تجلس طوال اليوم تفكر ماذا يجب أن افعل فتجد نفسك تتنقل بين الفايس بوك وتويتر واليوتيوب والمنتديات وأنت مازلت تفكر ماذا يتوجب علي فعله ؟ وأنا مرت بي هذه التجربة منذ عامان تقريبا ومن خلالها تمكنت من فهم الطريقة المثلى في تنظيم الوقت , تجربتي كانت في أول أيام افتتاح المدونة فأنا كنت ملزما بالتحضير لكورس التربل شووت الجديد والتحضير لمشروع التخرج في الجامعة وإعطاء كورسات تعليمية لبعض الطلاب وكتابة تدوينة بشكل شبه يومي ومتابعة منتدى عرب هاردوير وتصميم المجلة وتنسيقها (هذه المرحلة كانت بالنسبة لي المرحلة الذهبية في أستغلال الوقت) وطبعا كنت أعاني من ضغط رهيب في تحديد مهامي ولكن تمكنت من حل المشكلة من خلال طريقة بسيطة جدا وهي الورقة والقلم ولكن هذه المرة لا أكتب برنامجي اليومي كاملا , لا أبدا , أكتب واجباتي التى يجب أن أقوم بها غدا وقبل أن أنام وألصقها على شاشة الكمبيوتر وهي عادة تكون على الشكل الآتي :

قراءة جابتر من كتاب تربل شووت , كتابة تدوينة , عرب هاردوير , التحضير للكورس الأول , الرد على رسائل البريد , التحضير للدرس الثاني , عرب هاردوير , رسالة التخرج , المجلة .

قد تعتقد أن المهام كثيرة ولكن صدقوني لايمر يوم أنظم فيه مهامي بهذه الطريقة إلا وأنفذها جميعها والحمد لله وأكيد أذكركم أن هذه المرحلة في حياتي كانت مرحلة ذهبية ملكت طاقة لا أعلم مصدرها لكن أكيد من عند الله , وأدعوك لتجربتها من اليوم أكتب لنفسك المهام التى تريد تنفيذها غدا ولاتقيد نفسك بالتوقيت لأنك سوف تخسر كل مخططك وأجعل كل مهامك إيجابية , قراءة عشر صفحات من كتاب , قراءة خمس مقالات في الشبكات , الإجابة على خمس اسئلة تقنية موجودة على المنتديات , كتابة مقال للمجلة , مشاهدة فيديو تقني عن سيسكو , والخ . . . أختر لنفسك بعض المهام لكن احرص أن تكون كلها إيجابية لان باقي وقتك سوف يضيع في السلبيات لذلك لاتكتب شيئ سلبي مثل فايس بوك والخ . . .

وآخيرا تنظيم الوقت قد يكون شاقا لو أتبعت نظام الساعات والاوقات لكن لو حددت مهامك على الورقة والقلم واشدد على هذه النقطة «ورقة وقلم» حينها فقط سوف ترى أن وقتك بالفعل بدأ يستغل بشكل أفضل , لأن لو قررت أن أؤدي مهمة واحدة من مهامي بدون تخطيط مسبق لها فأنا سوف أنجح في تنفيذها لكن سوف أستغل يومي كاملا في تنفيذها لأن عدم وجود مهام آخرى في رأسي سوف يجعلني أتقاعس وأبدد وقتي في تنفيذ مهمتي الوحيدة وعندما أنتهي منها أحتاج وقت آخر لتحديد المهمة الثانية وهو مايجعلنا لانستثمر بوقتنا بشكل كافي وأنهي معكم بمقطع مصور شاهدته منذ فترة عن قيمة الوقت , يبدأ المقطع بسؤال صغير تصور لو أن هناك بنك يعطيك كل يوم 86400 دولار ويشترط عليك البنك القيام بصرف المبلغ كاملا فهل سوف تصرفه كله ؟ ويشترط عليك ايضا نقطة صغيرة وهي لو في حال لم تتمكن من صرفه فباقي المبلغ سوف يذهب منك , فهل أنت قادر على صرفه ؟ والأجابة أتركها لك فهو طبعا يقصد بالرقم عدد الثواني الموجودة في اليوم وهو الكنز الذي لديك ولابد لك من إتقان طريقة التعامل معه فهل أخذت ورقة وقلم الآن وبدأت تسجل مهامك !.ودمتم بود .

أيمن النعيمي - سوريا



مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

أسـرة المجلـة

المؤسس و رئيس التحرير

م.أيمن النعيمي

المحـررون

م.نادر المنسي	م. شريف مجدي	---
م.خالد عوض	م. أحمد هيكل	---
م.علاء معن الشوا	م.أنس المبروكي	---
م.نادر المنسي	م. تميم حميش	---

التصميـم و الاخـراج الـفني : محـمـد زرقـة

مدقق أملائي ونحوي للمجلة : عثمان اسماعيل

جميع الأراء المنشورة تعبر عن وجهة نظر الكاتب ولا تعبر عن وجهة نظر المجلة

جميع المحتويات تخضع لحقوق الملكية الفكرية و لا يجوز الاقتباس أو النقل دون اذن من الكاتب أو المجلة

www.networkset.net



- الفهرس 4
- Risc and Sisc 6
- كيف تحمي شبكتك (الجزء الثاني) 8
- أكثر المهارات المطلوبة في قطاع التكنلوجيا لعام 2012 11
- تعرف على شركة Nortel 12
- What happen if BLV is lost 20
- حماية الشبكات اللاسلكية من صواعق البرق 21
- ماهي خاصيةIP Service Level Agreement 26
- تقنيات AirMagnet 31
- أهم عشرة أشياء يجب أن تعلمها للمستخدمين 35

NetWork Set

معنى جديد لعالم الشبكات في سماء اللغة العربية

Magazine NetworkSet

أول مجلة عربية متخصصة
في مجال الشبكات

NetworkSet

مدونة عربية متخصصة
في مجال الشبكات

Wiki.NetworkSet

أول موسوعة عربية حرة
و متخصصة في مجال الشبكات



أول مشروع عربي لترجمة
المواد العلمية و التقنية

YouTube

قناة المدونة على يو تيوب



قسم خاص بالأسئلة والاجوبة



RISC AND CISC

لماذا اليونكس لا يعمل على الأجهزة الشخصية PC؟

كم هي كثيرة توزيعات اليونكس واللينكس وعندما تظهر أي توزيعه جديدة يبدأ التساؤل هل هي جيدة؟ وما هي التطورات التي أدخلت عليها؟, لكن التساؤل الذي لم يخطر على بال الكثير منا وهو لماذا نستطيع تشغيل توزيعات مثل Ubuntu على الأجهزة التي نمتلكها من PC & Laptop بينما لا نستطيع تشغيل توزيعات مثل Unix AIX على الأجهزة التي نمتلكها؟, وإليك الجواب:

كما نعلم جميعا أن هناك structure أو بناء خاص بالمعالج الموجود في الأجهزة والتي على أساسه يتم تحديد كيفية تعامله مع نظام التشغيل الموجود عليه, وهذا البناء أو التقنية المستخدمة تنحصر فى تقنيتين وهما RISC & CISC وهنا تكمن الاجابه .

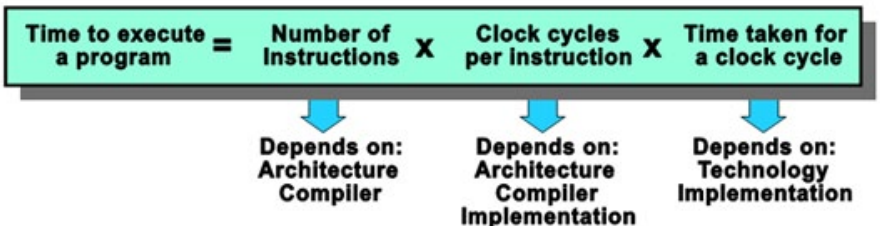
ولكن فى البداية لنتعرف على ماهية كل تقنية من هؤلاء:

1 - CISC : Complex Instruction Set of Computing

وهى التنقية المستخدمة في معالجات Intel & AMD أي الموجودة في الأجهزة التي نمتلكها وفيه يقوم المعالج بأخذ جميع Instruction من نظام التشغيل الموجود عليه ويقوم بمعالجتها أي أنه يقوم بمعالجة عدد كبير من البيانات والأوامر لذلك يسمى معقد Complex .

2 - RISC : Reduced Instruction Set of Computing

كما هو واضح من الاسم Reduced Instruction أي أنه تم تخفيض عدد الأوامر التي يقوم المعالج بمعالجتها, وهنا في الغالب يكون بوجود Compiler فيقوم بتخفيض عدد الأوامر التي تصل من نظام التشغيل إلى المعالج وبالتالي يكون الوقت المستهلك من قبل المعالج في معالجة الأوامر والبيانات أقل .



لتوضيح هذا الفرق دعنا نقوم بعمل المثال الآتي :

المعادلة التي تحكم الوقت المستهلك من قبل المعالج فى معالجة البيانات هي كالآتي :

```
Time taken = No. of instruction* cycle per Inst. *
time taken by every cycle
```

RISC AND CISC

دعنا نفترض الآتي, أنه لتنفيذ كل أمر يأخذ المعالج دورة Cycle واحدة وتأخذ وقت قدره ثانية واحدة.
في حالة CISC نفترض أن المعالج عليه معالجة 150 أمر وبالتالي يكون الوقت المستهلك كالآتي :

```
Time taken = 150 * 1 * 1= 150 sec = 2.5 minutes
```

في حالة RISC لا يقوم المعالج بمعالجة 150 أمر ولكنه يقوم بتخفيضه إلى عدد أقل, ولنقل مثلا إلى 60 أمر على سبيل المثال فيكون الوقت المستغرق كالآتي :

```
Time take = 60*1*1 = 60 sec = 1 minute
```

أي أنه أقل من الوقت الذي تم فيه تنفيذ نفس عدد الأوامر والبيانات في حالة CISC .

لذلك رأت الشركات التي تنتج اليونكس مثل :
IBM : AIX UNIX
HP : HP-UNIX
ORACLE : ORACLE SOLARIS
أن تصنع أجهزة خاصة بها تعمل على RISC, وكذلك نظم اليونكس الخاصة بها لا تعمل إلّا على هذه Platforms الخاصه بها .

بعكس توزيعات اللينكس المختلفة التي تعمل جميعها على CISC, وبالتالي تعمل جميعا على منصات INTEL & AMD وبالتالي نستطيع عمل Virtual Machine منها واستخدامها بكل سهولة .

وإن كان هناك نسخة من السولاريز تعمل على المنصات انتل أي أننا نستطيع استخدامها على الأجهزة الشخصية.

وايضا مع التقدم العلمي الحادث إلى الآن في التقنيتين لا استطيع أن أقول بأن هناك فرق كبير بينهما, حيث أن التكنولوجيا تقدمت بشكل يجعل كل من التقنيتين يقوم بمهامه بالشكل المطلوب .



كيف تحمي شبكتك
الجزء الثاني

هذا هو الجزء الثاني لكيف تحمي شبكتك ,في الجزء السابق تحدثنا عن بعض الهجمات التي من الممكن أن تؤثر على عمل الشبكة أو يكون لها تأثير سلبي ,خلال هذا الجزء سنتعرف على أنواع أخرى من الهجمات وطرق التصدي لها على أجهزة سيسكو .

التصدى لهجمات التزوير MAC Spoofing

هجمات التزوير Mac Spoofing تعتمد على خلق إطارات Frames تحتوي على عناوين فيزيائية مزيفة وإرسالها إلى الـ Switch, قد يكون ذلك لأغراض كثيرة, لذلك يجب تأمين منافذ الـ Switch بحيث يمكنها التعرف على هذه البيانات المزيفة وحجب مرسلها, بالطبع يكون إعداد ذلك على الـ Switch بهذه الطريقة

```
SW1(config)#interface fa010/
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 1
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#switchport port-security violation shutdown
```



الأوامر السابقة تقوم بتفعيل خاصية تدعى port security وهي موجودة على أغلب السويتشات وليست خاصة بسيسكو فقط , أولا يجب تفعيل الخاصية بأمر switchport port-security وهو ضروري لكي تعمل هذه الخاصية, بعد ذلك يتم تحديد أقصى عدد من العناوين يمكن استقباله على منفذ معين وبالطبع يساوي 1 لأننا نتوقع أن يكون كل منفذ متصل بجهاز واحد _إلا في حال إذا كان المنفذ متصل بـ HUB, بعد ذلك نُدخِل الأمر switchport port-security mac-address sticky وهو يخبر السويتش أن يقوم بتحديد العناوين الصحيحة عن طريق أول Frame تصل إليه, فيقوم بلصق الـ Source MAC على هذا المنفذ ولا يستقبل شيء من أي مصدر آخر , الأمر الأخير switchport port-security violation shutdown يقوم بتحديد الإجراء الذي يتم اتخاذه في حال تم استقبال عناوين مزيفة, والإجراء الذي سيتم فرضه هو إغلاق المنفذ نهائيا في حال حدث أي انتهاك .

التصدي لهجمات بروتوكول DHCP

إذا كان لديك في الشبكة DHCP Server فلابد أن تعرف بعض الهجمات التي يمكن تطبيقها عن طريق هذا البروتوكول ,على سبيل المثال يمكن أن يقوم شخص ما باستخدام أحد البرامج بتشغيل جهازه كـ DHCP Server مزيف و يقوم بالتصنت على طلبات الحصول على عناوين وبعد ذلك يقوم بإرسال عناوين غير صحيحة , قد يُمكّن هذا المخترق من فعل الكثير في الشبكة, ويمكن التصدي له بتنفيذ الأوامر التالية :

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#int fa024/
SW1(config-if)#ip dhcp snooping trust
```

الأوامر السابقة تقوم بتفعيل خاصية تسمى DHCP Snooping وهي تعمل على السويتشات, الأمر الأول والثاني عملهم هو تفعيل الخاصية وتحديد الـ VLAN المطلوب تفعيل الخاصية عليها ,بعد ذلك نذهب إلى المنفذ المتصل بالـ DHCP Server الحقيقي ونقوم بتحديده كـ Trust أي منفذ موثوق لتوزيع العناوين ,أما باقي المنافذ فتكون By Default غير موثوق بها Untrust, وبذلك إذا وجد السويتش أي شخص يحاول الرد على طلب الحصول على عنوان DHCP Request فإنه يقوم بمنع الرد, باستثناء إذا كان الرد مصدره منفذ موثوق به Trusted, غير ذلك يتم منعه .

التصدي لهجمات التزوير ARP Spoofing



الـ ARP Spoofing هو القيام باستغلال بروتوكول ARP لعمل ARP cache poisoning وذلك عن طريق إرسال رسائل ARP مزورة إلى هدف معين ,لذلك كان يجب أن يقوم السويتش بالتحقق من العنوان الفيزيائي و الـ IP المقابل له في رسائل الـ ARP والتأكد من صحتها وأنها غير مزورة ,يمكن للسويتش التحقق من ذلك بالرجوع إلى جدول يحتوي على العنوان الفيزيائي لكل جهاز وعنوان الـ IP الصحيح ,يتم تغذية هذا الجدول من خلال الخاصية السابقة DHCP Snooping حيث يتم تسجيل ذلك من خلال طلبات الـ DHCP, الخاصية التي تقوم بعمل هذا الفحص لرسائل الـ ARP تسمى Dynamic ARP inspection (DAI) ويتم تفعيلها بهذه الطريقة

```
SW1(config)#ip arp inspection vlan 1
```

بالطبع يجب أن تكون خاصية DHCP Snooping تم تفعيلها مسبقا قبل تفعيل الـ DAI .



التصدي لهجوم VLAN Hopping

أحد أهداف الـ VLAN هي عمل تقسيم على مستوى الطبقة الثانية Layer 2, ومن فوائد هذا التقسيم هي فصل كل VLAN عن الأخرى ,ففي حال تم وضع مجموعة من الأجهزة في VLAN يجب التأكد من أن هذه الـ VLAN مفصولة عن غيرها ,إلا أن هناك بعض الحيل تُمكّن المستخدمين من الوصول إلى VLAN غير التي ينتمون إليها ,فكرة هذا الهجوم تعتمد على الـ Native Vlan والقيام بعمل Double Tagging يكون الخارجي منها هو الـ Native VLAN والداخلي منها هو الـ VLAN المرغوب الوصول إليها ,وعندما تبدأ هذه الـ Frame في عبور الـ Trunk يتم إزالة الـ Tag الخارجي لأنه يحتوي على الـ Native VLAN فيتبقى الـ Tag الداخلي ,ولمنع هذا الهجوم يتوجب عليك تطبيق الآتي :

```
SW1(config)#interface fa019/
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 10
```

ما تم تطبيقه عن طريق الأوامر السابقة هي تحويل الـ Native Vlan إلى واحدة غير مستعملة .

التصدي لهجوم حجب الخدمة DOS Attack

ماذا يحدث إذا انتشرت في الشبكة Worm تقوم بالتسبب في حجب الخدمة عن FTP Server عن طريق إنشاء عدد كبير من الـ Half-open-session تمنع المستخدمين من الوصول إلى السيرفر ,بالطبع يسبب هذا الكثير من المشاكل بغض النظر عن نوع السيرفر سواء كان ويب أو FTP, الطريقة التالية توضح كيفية التصدي لذلك باستخدام الـ ASA لحماية سيرفر FTP , إلا أن نفس الطريقة يمكن تطبيقها مع أي بروتوكول آخر

```
ASA(config)# class-map FTP
ASA(config-cmap)# match port tcp eq ftp
ASA(config)# policy-map FTP
ASA(config-pmap)# class FTP
ASA(config-pmap-c)# inspect ftp
ASA(config-pmap-c)# set connection embryonic-conn-max 1000
ASA(config)# service-policy FTP interface inside
```

هذه الأوامر ما هي إلا تطبيق لمفهوم Modular Policy Framework أو MPF والذي يستخدم للتحكم في تدفق البيانات عبر الـ ASA وطريقة فحصها , في البداية تم إنشاء Class map تقوم بعمل Match للترافيك المطلوب وفي هذه الحالة اخترنا الـ FTP, بعد ذلك يتم إنشاء Policy Map لتحديد الإجراءات المطلوبة على الـ Class Map التي قمنا بإنشائها ,وتم تحديد الحد الأقصى من الـ embryonic-conn-max لمنع زيادة عدد الـ Half-Open- Session .

أتمنى إن أكون قد ساهمت في تقديم شيء جديد وإلى لقاء آخر في عدد جديد فمازال هناك الكثير .

أكثر المهارات المطلوبة في قطاع التكنلوجيا لعام ٢٠١٢



منذ شهر تقريبا كنت قد نشرت على تويتر مقالة أجنبية عن أكثر عشر مهارات سوف تكون مطلوبة في مجال تقنية المعلومات في العام القادم 2012 وفق دراسة وإحصائية قام بها موقع techrepublic, ولأهمية المقال وجدت ترجمته شيء مفيد وهام للباحثين عن مجالات جديدة في قطاع التكنلوجيا .

1. البرمجة وتطوير التطبيقات "61٪ " هي نسبة استئجار هذه المهارة في الأشهر الـ 12 المقبلة ، صعوداً من 44٪ مقارنة باستطلاع عام "2010. تغطي هذا السلسلة نطاق واسع , تبدأ من تطوير الموقع لتحسين الأنظمة الداخلية وتلبية احتياجات مستخدمي الهواتف المتحركة.
2. إدارة المشاريع (ولكن مع تطور) – ويقصد بـ " تطور" أي أنّهم لن يكونوا مجرد باحثين عن الأشخاص الذين يمكنهم مراقبة ورصد المشاريع, بل إنّهم يريدون أيضاً الأشخاص الذين يمكنهم التعرف على احتياجات المستخدمين وترجمتها إلى ما يفهمه عاملي تكنولوجيا المعلومات .
3. مكتب المساعدة، الدعم التقني وأنظمة تشغيل الأجهزة المحمولة قد أضافوا بُعداً جديداً لمكتب المساعدة التقنية والدعم
4. .الشبكات، هذا هو الطلب الذي يتم تغذيته جزئياً من خلال تقنية الـ Virtualization ومشاريع الحوسبة السحابية. وكشفت الدراسة أيضاً أنّ المدراء سيبحثون عن الأشخاص بواسطة "VMware" وتجربة سيتريكس.
5. . الذكاء التجاري وعالم الحواسيب يفسر هذا التنامي في تحويل التركيز في العديد من الشركات، من الاهتمام بتقليل التكاليف إلى الاهتمام في الاستثمار في التكنولوجيا. وسوف يكون لطيفاً لو سار الأمر على هذا النحو.
6. . يمكن أن تكون مراكز البيانات التخيلية من خلال تقنية الـ Virtualization ،والحوسبة السحابية وراء ازدياد الحاجة لمتخصصي تكنولوجيا المعلومات من ذوي الخلفيات والخبرة في عمليات مراكز البيانات وتكامل النظم



7. . مهارات تقنية "Web 2.0" والتي تتمحور حول وسائل الإعلام الاجتماعية ستكون مطلوبة. "PHP"، "AJAX"، "Net"مطلوبة كمهارات رئيسية مع ، CSS ، XML ، HTML Flash وجافا سكريبت ،مطلوبة من بين أمور أخرى، على الواجهة الأمامية.
8. . الأمن والحماية، على الرغم من انخفاض الاهتمام به بنسبة 32 ٪ مقارنة باستطلاع عام 2010 ، إلّا أنّه يبقى مصدر القلق الأكبر للمسؤولين التنفيذيين لتكنولوجيا المعلومات.
9. . الاتصالات السلكية واللّاسلكية، يشير المسح إلى وجود حاجة لذوي مهارات الاتصال عبر بروتوكول الإنترنتIP telephony ، وكذلك الأمر بالنسبة لأولئك المتعاملين مع أنظمة مركز الاتصال "سيسكو IPCC ".



أحببت اليوم في مقالتي الثانية أن أستعرض للقراء الكرام معلومات عن شركة Nortel ، ربما الكثير لم يسمع عنها لأنها ليست بعد على مستوى أو انتشار الشركات الكبرى مثل (Cisco, Juniper, 3COM) ولكنها تقدم حلا مميزا من ناحية الأداء وبسعر مقبول جدا قد يدفعك للتفكير في اقتناء أحد منتجاتها ...

لمحة عن تاريخ الشركة :

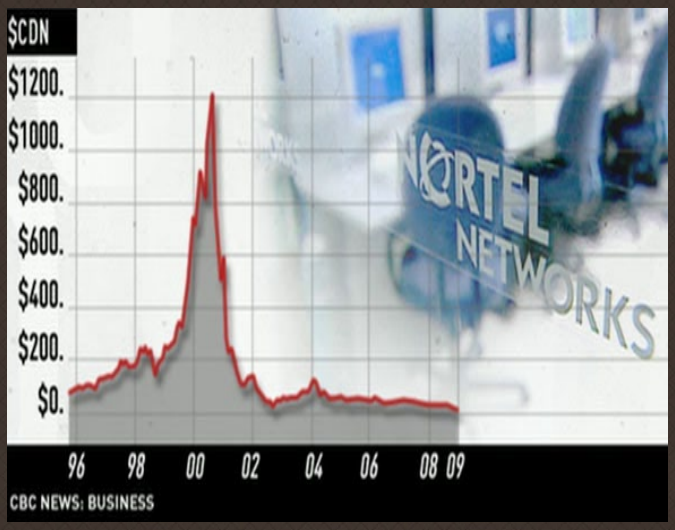
تمتلك الشركة تاريخا حافلا في تجهيزات الاتصالات حيث يعود أصلها لشركة (Bell Telephone Company) وهي شركة كندية تأسست عام 1882م وتطورت هذه الشركة منذ ذلك الوقت حيث كانت متخصصة فقط في معدات الاتصالات الهاتفية التقليدية إلى أن أصبح اسمها (Northern Electric and Manufacturing Company)

لن أطيل كثيرا في مراحل تطور الشركة ولكن هذا الاسم الأخير هو الذي أدى إلى إبصار (Nortel Networks) النور عام 1995م ، ومنذ ذلك الوقت و (Nortel) تقوم بمشاركة كبرى الشركات العالمية لإبراز اسمها كأحد أقوى المنافسين على مستوى آسيا وكندا وحتى أمريكا

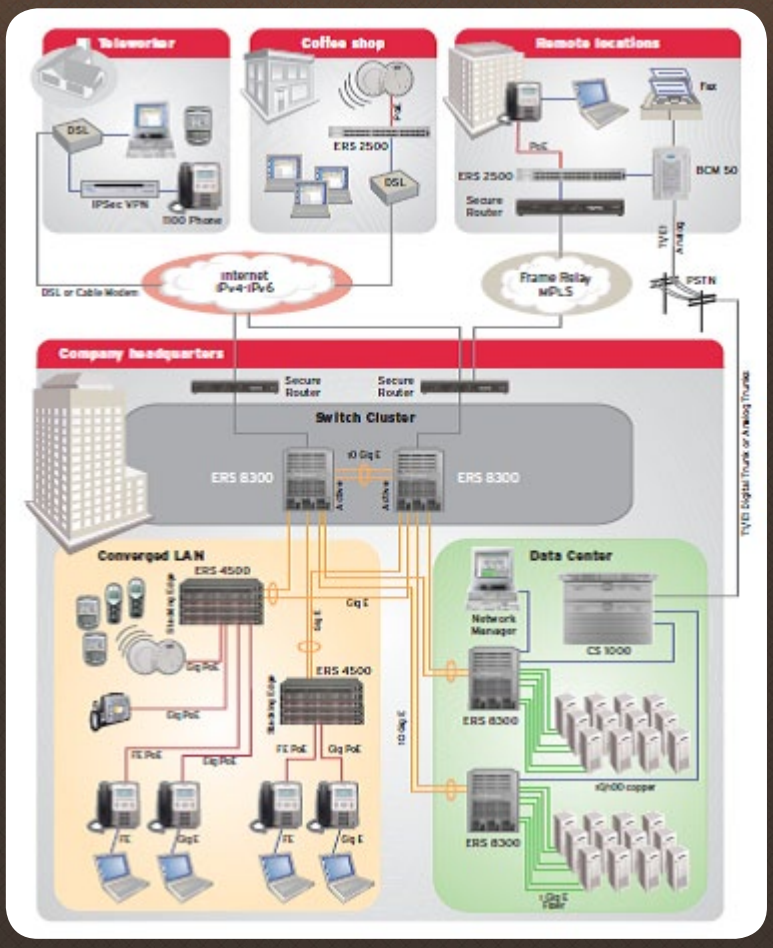
منتجات Nortel :

تنتج الشركة المعدات والبرمجيات الخاصة بكل ما يلي :

1- LAN, MAN & WAN
2- Phones, Clients & Accessories
3- Voice, Multimedia & Unified Communications
4- Optical Networks
5- Security & VPN
6- Wireless Networks







الشكل (1)

سنسلط الضوء على بعض المنتجات والدعم البرمجي لها والمزود بواجهات رسومية لسهولة الاستخدام.

المبدلات (السويتشات) Switches:



الشكل (2)

وتشمل عائلة ضخمة تلبي جميع الاحتياجات من المكاتب الصغيرة ومقاهي الإنترنت إلى الشركات الضخمة التي تمتلك مئات بل وآلاف الطرفيات ، ومنها الموديلات (ERS 3510, ERS 4500, ERS 5500 and ERS 8600). ما يميزها جميعها بأنها ليست (Switch) فقط، بل هي (Routing Switch !!)، بمعنى آخر تصور أخي القارئ أنك ستمتلك جهاز (Switch) كأي جهاز من شركة أخرى بكامل قدرات الـ (Switch) ولكنه يستطيع التعرف على بروتوكولات الطبقة الثالثة وذلك بواسطة البرمجية التي تقدمها الشركة والتي تدعم هذا الجهاز حيث سأتحدث عنها لاحقا.

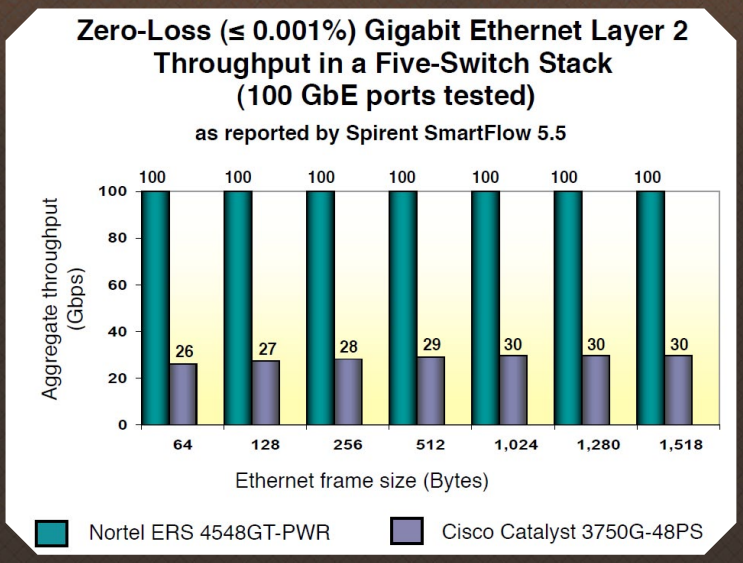
الجدير بالذكر أن عائلة الـ (ERS 8600) تستثنى من الكلام السابق لأنها أصلا أجهزة (Core Switch) وهي بشكل طبيعي تعمل في الطبقة الثالثة (Layer 3) حالها كحال جميع الـ (Core Switches).

1 -عائلة (ERS 4500):

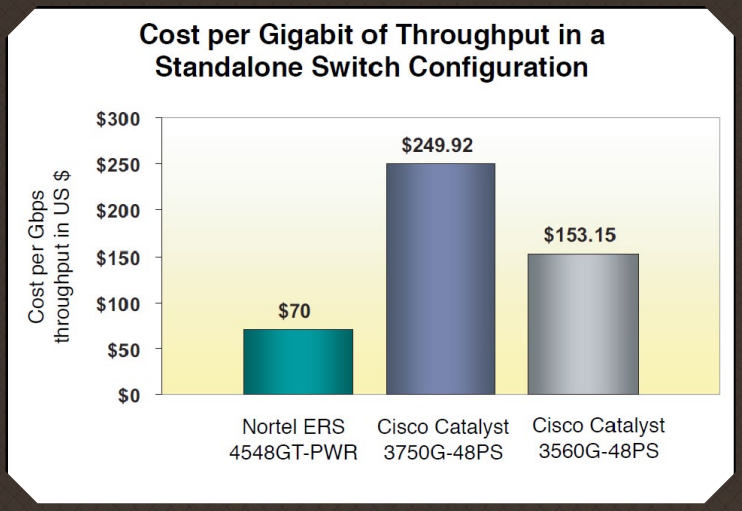
وقد قمت باختيار الموديل (ERS 4548GT PWR) والموضح بالشكل، حيث يأتي بـ 48 منفذ بسرعة 1000/100/10 BaseTX إضافة لميزة (PoE) أي نقل الطاقة عبر الـ (Ethernet) مع وجود أربع منافذ (Shared SFP Ports) وهنا بعض الميزات الفنية :

- Total stacking capacity: 320 Gbps
- Total packet throughput: 240 Mpps
- Individual switch capacity: 48.8 – 184 Gbps
- Concurrent VLANs: 256
- Maximum MAC addresses: 8,000

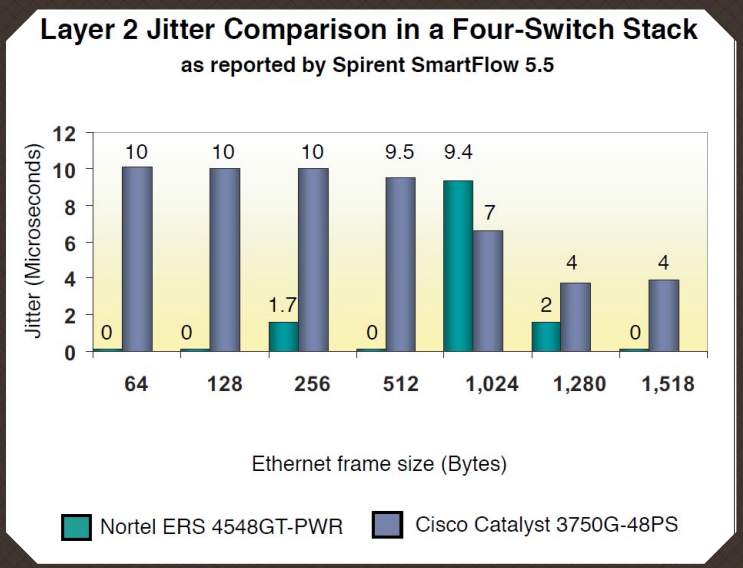
وحسب ما ذكر موقع (Tolly) أو ما يعرف بـ (Tolly Group) المتخصص في الاختبارات، قام بعمل مقارنة مع الموديل الشهير (Catalyst 3750G-48PS) من شركة (Cisco)، حيث قام بعمل عدة اختبارات ومقارنات من جميع النواحي والتي سأستعرضها بالصور التالية وأترك الحكم لكم:



الشكل (3)



الشكل (4)



الشكل (5)

2 - عائلة (ERS 8500):

في مثل هذه الأجهزة (أي الـ Core Switches) يتم تحديد قوة الشركة وقدرتها على تصنيع منتجات عالية الدقة، لأن مثل هذه التجهيزات تستخدم في ربط كم هائل من البيانات لعدة مواقع وبسرعات عالية جدا، فيتبين لدينا إن كانت الشركة قادرة على تخديم مثل هذه العملية دون أخطاء وبوثوقية وسرعة عالية، وهنا اعذروني ان كانت خبرتي قليلة في مجال الشبكات لأن التعامل مع مثل هذا النوع من التجهيزات لا يتوفر إلا لدى الشركات الضخمة والتي تمتلك مئات الطرفيات في عدة مواقع. وسنستعرض الموديل (ERS 8610 Resilient Terabit Switch) وبعض الميزات التي يدعمها هذا الجهاز:

Core converged networking:
> IP Telephony
> Wireless LAN
> Data Center
> Wire speed IPv6
> Wire speed IP Flow Information eXport
> SMLT with sub 100ms convergence
> High Scalability Multi-Cast
> Integrated Service Delivery
:

أما بالنسبة للمواصفات التقنية فهي:

- 48-port 101000/100/BaseT auto-speed Sensing
- 30-port 1000 SFP GBIC
- 3-port 10 Gigabit XFP LAN PHY
- 3-port 10 Gigabit XFP LAN/WAN PHY
- R-Modules require 8692SF

- Additional modules:
- 32-port 10100/BaseTX
- 24-port 100BaseFX
- 16-port 1000BaseT
- 8-port OC-3 ATME
- 2-port OC-12 ATME

- 8-port 1000BaseSX
- 8-port 1000Base GBIC
- 8-port 1000BaseT

الذي يميز هذا الجهاز هو سعره، فهو ذو مواصفات تقابل الجهاز (Cisco 6509) ولكن بسعر يصل إلى نصف سعر جهاز (Cisco) !! إضافة إلى أن (Tolly Group) أكدت تفوقه في بعض الاختبارات.
بشكل عام لو كان لي الخيار والميزانية مفتوحة فبالطبع سأختار (Cisco) دون تردد لسبب وحيد أنني لن أضع نفسي في المجهول، ولكن لو تمت المقارنة مع أخذ الميزانية بعين الاعتبار لاخترت (Nortel 8610) دون تردد، فأنا شخصيا معجب بهذا الجهاز والمهندس المختص في الشركة التي كانت تحوي هذا الجهاز أثناء فترة تدريبي وتعاملي معه أكد لي أن الجهاز يعمل بكفاءة عالية جدا ودون اي أخطاء منذ 3 سنوات...

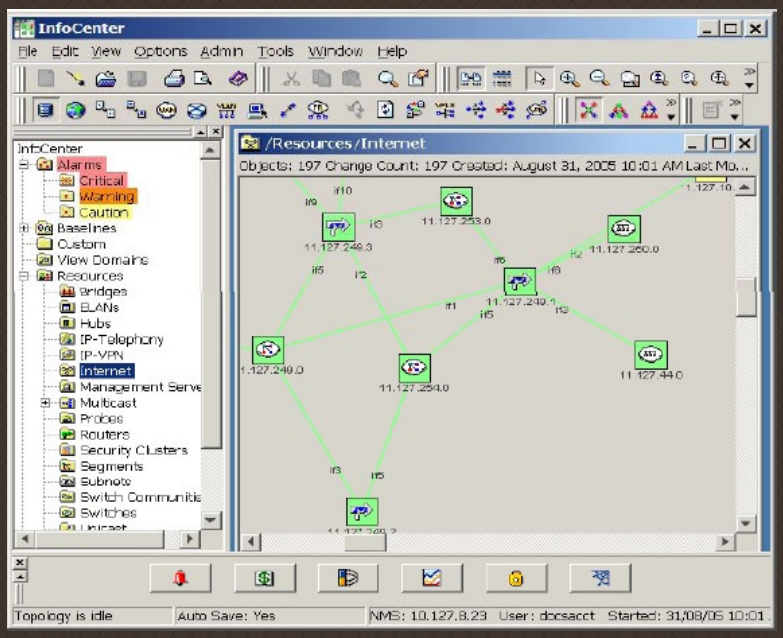


الشكل (6) ERS 8610

: ENMS (Enterprise Network Management System)

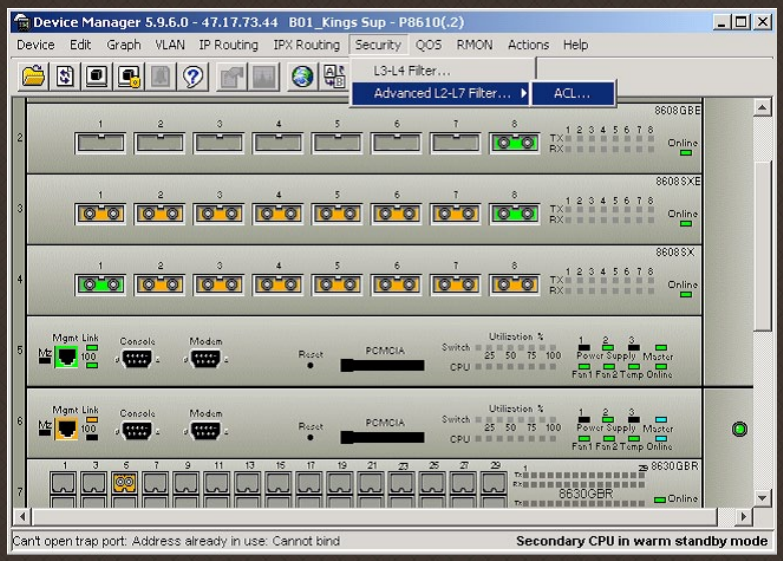
يشكل نظام إدارة الشبكة الواجهة الرسومية التي يتم التعامل معها ضمن بيئة نظام التشغيل والتي تمكن اختصاصي الشبكة من برمجة الأجهزة و مراقبتها في الزمن الحقيقي والكشف عن حدوث خلل في حال حدوثه... حيث تتلخص وظائف النظام وفق ما يلي:

- Security
- Fault Management
- Performance
- Configuration



الشكل (7) واجهة البرنامج الرئيسية

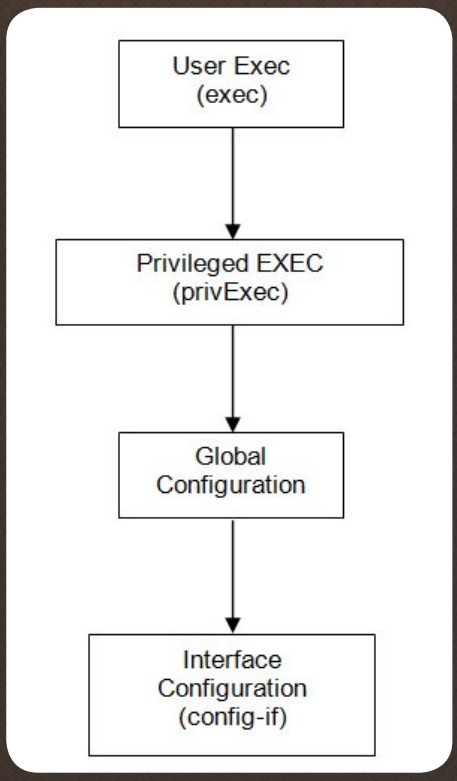
يتألف النظام من عدة إصدارات تختلف بحسب الحاجة المرغوبة (ENMS Server-ENMS Client-ENMS Database) ولكل إصدار مزايا وخصائص تختلف عن الآخر



الشكل (8) منافذ الجهاز ضمن البيئة البرمجية

يمتلك النظام واجهات رسومية مبسطة وسهلة تتيح التعامل مع الأجهزة، وكما نلاحظ في الشكل فإن الألوان تلعب دور لتحديد وضع المنفذ في الجهاز في حال كان متصل أو خامل.

حيث يحتوي هذا النظام على الكثير من الخيارات والتي تحتاج ربما لعدد كامل لشرحها واستعراضها.



كيفية ضبط الإعدادات :

بالإضافة إلى الواجهة الرسومية التي يستطيع مهندس أو فني الشبكة ضبط الاعدادات فيها، تتوفر إمكانية استخدام الـ (Console) أو ما يعرف بالـ (CLI). وهنا سأسمي الطريقة التي تتم بها عملية برمجة الجهاز بـ «المألوفة» لأنها كذلك لدى كثيرين من الدارسين والملمين بعالم الشبكات وستكتشفون السبب بعد أن أستعرض بعض الأوامر

بداية سأوضح هذا المخطط والذي يبين التسلسل الهرمي لمستويات ضبط الاعدادات في الـ (CLI)

يتم الدخول إما عن طريق منفذ الـ (Console) الموجود في الجهاز، أو بواسطة الولوج عن بعد كما في الـ (Telnet) أو (SSH) ،وبعد الدخول سنلاحظ الرمز الذي يدل على كل مستوى كما يلي:

- User EXEC: Switch>
- Privileged EXEC: Switch#
- Global Configuration: Switch(config)#
- Interface Configuration: Switch(config-if)#

يتم الدخول إما عن طريق منفذ الـ (Console) الموجود في الجهاز، أو بواسطة الولوج عن بعد كما في الـ وللدخول من مستوى الـ (User) لمستوى الـ (Privileged) يكفي كتابة (enable)



كذلك من مستوى الـ (Privileged) لمستوى الـ (Global Configuration) نكتب (configuration terminal)
أصبح من الواضح الآن أن التعليمات هي تلك نفسها التي تستخدم في الـ (IOS) الخاص بـ (Cisco) وصراحة لا أمتلك خلفية واسعة فيما إذا كانت جميع الشركات كذلك وأن (Cisco) هي الماركة المسجلة لهذا النهج.
فعلى سبيل المثال لو أردنا مثلا جدول الـ (MAC Address) وذلك لمعرفة الـ (MAC) المتصل في الطرف المقابل للـ (Interface) الموجودة لدينا، فيكفي أن نكتب (show mac-address-table) في مستوى الـ (Privileged) أو في مستوى الـ (Global Configuration) ليظهر لنا ما يلي :

```
Switch(config)#show mac-address-table

Mac Address Table Aging Time: 400
Number of addresses: 13

    MAC Address      Source     MAC Address      Source
------------------ -------- ------------------ --------
00-00-81-9B-12-78 Trunk:  3 00-00-E2-13-38-38 Trunk:  3
00-00-E2-1F-9D-0D Trunk:  3 00-04-DC-6F-43-F4 Trunk:  3
00-09-97-89-82-C1 Trunk:  3 00-0C-F8-1A-0F-F8 Trunk:  3
00-0C-F8-61-00-01 Trunk:  3 00-0F-3D-E5-28-01 Trunk:  3
00-0F-6A-82-2E-C1 Trunk:  3 00-0F-6A-82-36-21 Trunk:  3
00-0F-CD-BF-1E-80           00-80-2D-6E-47-38 Trunk:  3
00-80-2D-6E-47-82 Trunk:  3 08-00-20-9F-F3-2C Trunk:  3
```

ولو أردنا مثلا قفل أحد الـ (Interface) الغير مستخدمة، نكتب التعليمة التالية (shutdown) في مستوى الـ (Interface Configuration) وبالتالي سيقفل المنفذ نفسه، أو كتابة (shutdown port <port number>) وبالتالي سيقفل المنفذ الذي سيتم وضع رقمه.
عند كتابة (?) في أي مستوى والضغط على زر (Enter) سيظهر لنا جميع التعليمات الموجودة ضمن هذا المستوى ...

في النهاية تشكل منتجات (Nortel) حلا مثاليا للشركات والمؤسسات التي تعاني من ضعف في القوة الشرائية أو من حظر للمنتجات الأمريكية كما هو الحال في بلدي، بينما كما أرى أنا بأنها شركة تفوقت إلى حد ما في منع احتكار الشركات الأمريكية لقطاع التكنولوجيا والذي لطالما دفعنا وسندفع ثمنه مستقبلا (ليس طويلا بإذن الله) الملايين بل ومليارات الدولارات..

Magazine
NetworkSet
First Arabic Magazine for Networks

ضع أعلانك معنا وساهم في
تطوير واستمرارية أول مجلة عربية متخصصة



انتشار واسع - تغطية شاملة

حزم اعلانية مختلفة تناسب جميع الاحتياجات

AIX BLV

boot logical volume





س : ماذا يحدث إذا فقدت الـ BLV «boot logical volume» على سيرفر اليونكس AIX ؟

سؤال يتم تكراره كثيرا في الحقيقة, لأنه في أغلب الحالات يكون السيرفر الذي يعمل على AIX Platform يكون في الغالب سيرفر أوراكل أو ساب, وهي تطبيقات غاية في الأهمية ويعمل عليها أغلب إن لم يكن كل موظفو الشركة, لذلك ففي حال حدوث أي أعطال وخاصة إذا كانت متعلقة بتوقف النظام وفقدان البيانات الموجودة عليه عندها سنضطر إلى استرجاع البيانات من الـ backup الخاص بها فهي عملية تستغرق وقت كبير وهذا غير مسموح به على الإطلاق .

الحل :

كل ما يجب عليك فعله في هذه الحالة هو إتباع الآتي :

1 - قم بإدخال اسطوانة النظام AIX Operating System CD

2 - قم بعمل إعادة تشغيل للسيرفر وعندما يبدأ اضغط على f5 لكي تبدأ maintenace mode ولذلك لكي تتمكن من إصلاح الجهاز بعيدا عن النسخة الأصلية الموجودة على الديسك, لأنه في مثل هذه الحالات تكون النسخة الموجودة في الـ RAM من الاسطوانة وليست من الهارد ديسك .

3 - اختار الاختيار الثالث من القائمة وهو كالتالي Enter Maintenace Mode

4 - قم بإنشاء BLV جديد كالآتي :

1 Mklv -t boot -y hd5rootvg

Crfs -v boot -d hd5 -g rootvg

كل ما يتم فعله هنا هو إنشاء BLV جديد مكان القديم بنفس المواصفات وهي كالآتي :

Logical Volume group: rootvg

Volume Name: hd5

File system type: boot files

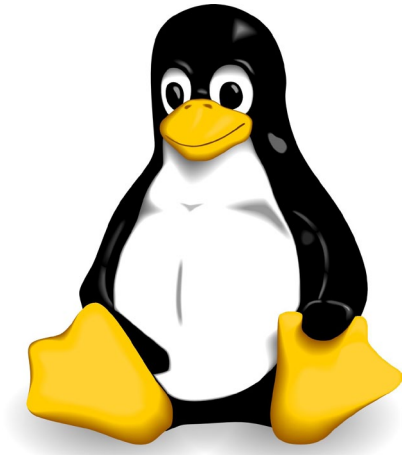
system size: 1 physical partition

5 - ثم بعد ذلك نقوم بتحديد الهارد الذي يوجد عليه BLV .

Bosboot -ad /dev/hdisk0

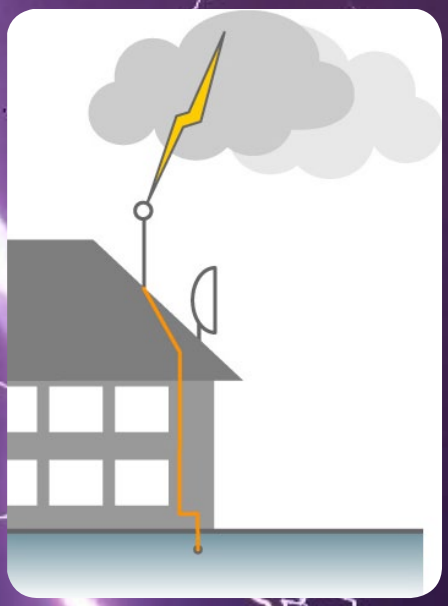
وهنا يفهم النظام أنه الهارد الذي يوجد عليه النسخة وهو hdisk0 والموجود في rootvg

6 - ثم بعد ذلك نعيد تشغيل الجهاز وفي خلال ذلك يقوم الجهاز بنقل الـ BLV الموجود على الاسطوانة إلى hd5 وهو BLV الموجود على الهارد ديسك وبالتالي يكون النظام أصبح في حالة ثبات .



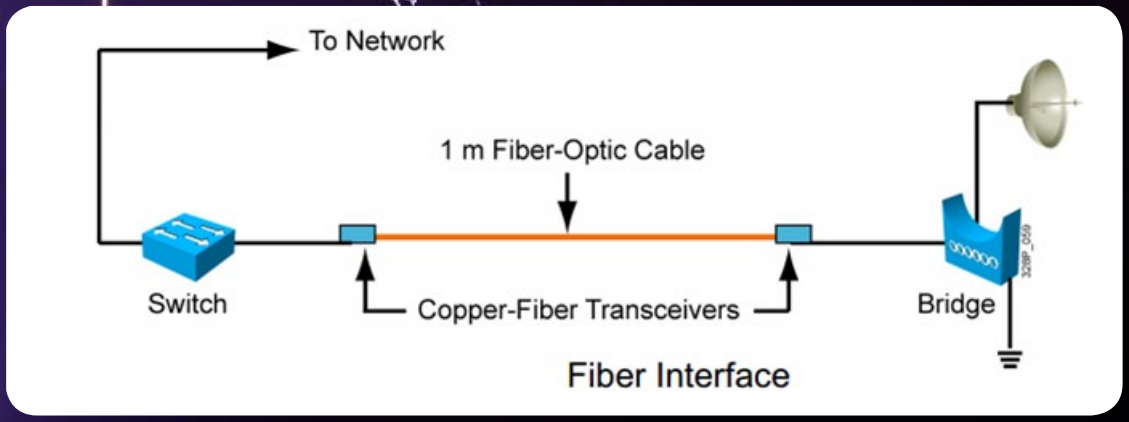
حماية الشبكات اللاسلكية من صواعق البرق



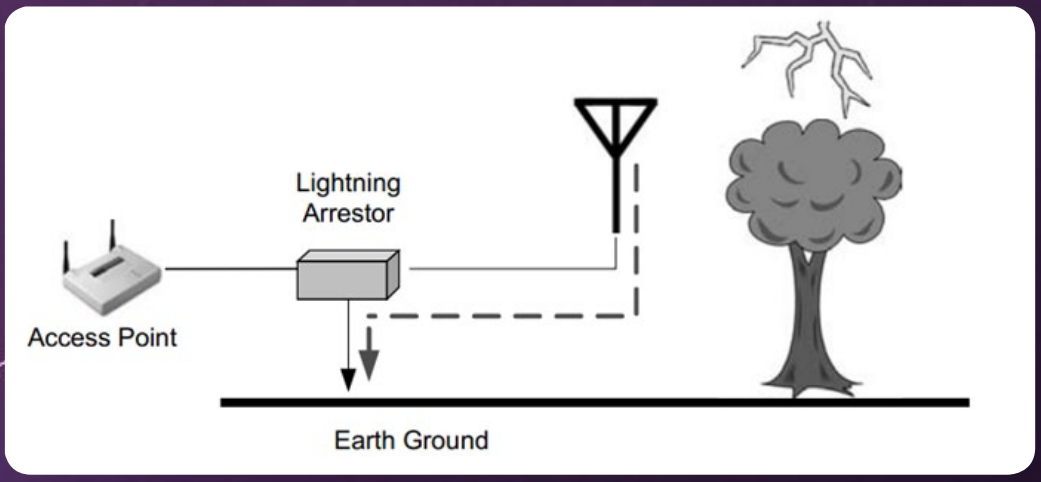


قد لا تعاني الشبكات اللاسلكية الداخلية Indoor من مؤثرات الجو و الطقس و البيئة حيث أنها تعتمد على الإشارة التي تتواجد داخل محيط مغلق , و لكن المشكلات كلها ستجدها عند تعاملك مع الشبكات اللاسلكية الخارجية Outdoor, حيث يتواجد عصب هذه الشبكة في العراء مثل الهوائيات و الكابلات التي تربط الهوائي بالجسر Bridge أو Access point بالإضافة إلى الإشارة نفسها التي تتواجد في الهواء.
كل هذه الأشياء أو بعضها تتأثر بكل العوامل الجوية أو بعضها, فالكابلات تتأثر فيزيائياً بالحرارة و البرودة فتتمدد و تنكمش و يتلف غلافها , و الهوائي يتأثر ميكانيكياً بالرياح و العواصف الرملية و الأمطار, فهذه الأشياء قد تزيحه أو تغير وضعه أو تؤثر في صقل سطحه و بالتأكيد كل هذا يزيد من قيم الفقد في الإشارة
لكن كل هذه المؤثرات تبقى معزولة عن الشبكة الداخلية و لا تؤثر في سلامتها و لا نعيرها اهتماما لأن التغلب عليها سهل و لا يستهلك وقت.
الخطر الأكبر في المؤثرات البيئية هي الصواعق الكهربية التي تصاحب العواصف و الأمطار و التي نعرفها باسم البرق Lightening , فالصواعق الطبيعية «البرق» هي أحد ألد أعداء الأجهزة الإلكترونية, فنادرا ما يحدث برق إلّا و تسمع في مكان ما عن تعطل في بعض الأجهزة أو تلفها بشكل تام
فبمجرد حدوث البرق بالقرب من هوائي الشبكة حتى يتأين الهواء المحيط بالهوائي – أي يصبح الهواء موصل جيد للكهرباء- فينتقل تيار كهربائي عالي إلى الكابل المتصل بالهوائي و منه يصل إلى أجزاء الشبكة و يعيث فيها فسادا كالذئب الذي وجد غنما ضالة.
و بالطبع هناك حلول

الحل الأول: هو عزل الهوائي كهربيا عن الشبكة باستخدام كابل فايبر قصير يربط كابل الهوائي بكابل الأكسس بوينت , فكما نعرف مسبقا أن من خصائص كابلات الفايبر أن الإشارة داخلها تنقل الضوء و لا تتأثر بالكهرباء و هذا يجعلها أكثر أمناً عند تمديد الكابلات بجوار كابلات ضغط عالي

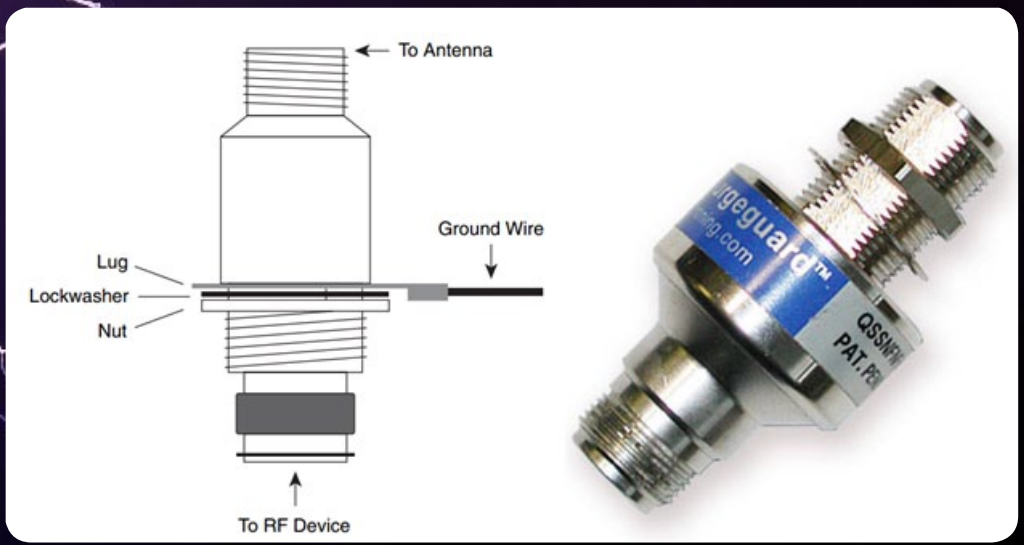


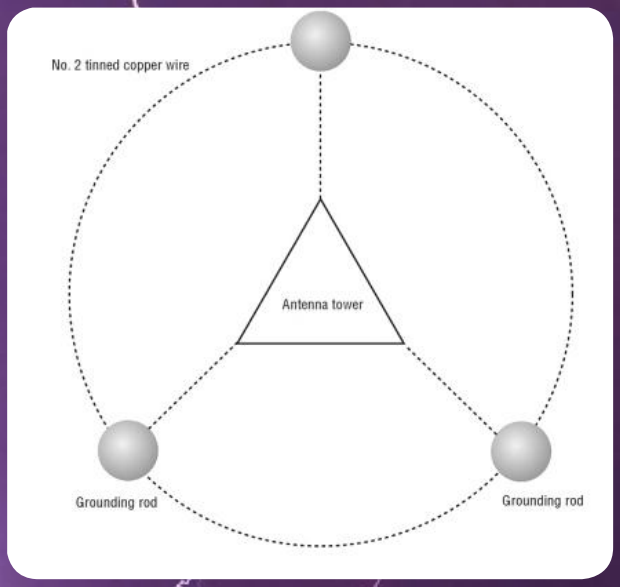
و رغم أنّ هذه الطريقة تحد بشكل شبه كامل و دائم من خطر الصواعق الكهربية للبرق من خلال العزل الكهربي الكامل إلّا أنها مكلفة لتطلبها محولات إشارة Ethernet-to from-fiber convert على نهايتي كابل الفايبر بالإضافة إلى تكلفة التركيب و الربط و التي لا يجيدها إلّا الفنيين المتخصصين.
و الحل الثاني: هو استخدام جهاز مانع الصواعق Lightning Arrestors و الذي يستطيع أن يحمي الشبكة من صواعق تصل قيمة جهدها فيما لا يزيد عن 50 فولت.



و هو يقوم بحماية الشبكة من الصواعق التي تمر بالقرب منه و التي تثير تيار ينتقل إلى الهوائي من تأين الهواء المحيط بالهوائي, حيث يقوم بتمرير – shunt- هذا التيار إلى منظومة التأريض و ذلك في فترة زمنية تعادل 100 نانو ثانية, و هو بذلك أسرع عشر مرات من سرعة ضرب البرق و هي 2 ميكرو ثانية.

فعندما يضرب البرق أي هدف أو يصيبه حثياً بالتأين فإنّ الشحنات الكهربية تسلك الطريق الأقل مقاومة كهربيا و هذه هي فكرة عمل lightning arrestor, حيث يقوم بتحويل الشحنات الكهربائية إلى المسار الأقل مقاومة من ثم إلى كابل متصل بالقضيب الأرضي Grounding Rods بعيدا عن أجهزة الشبكة, أي أن مانع الصواعق هذا يلعب دور Fuse في الأجهزة الكهربية





و لهذا فإن مانع الصواعق هذا لا يعمل إلّا في وجود نظام تأريض خاص يساعد على تحويل الشحنات الكهربية إلى الأرض بدلا من دخولها إلى الشبكة
حيث يتم ربط كابل في مانع الصواعق و مده إلى قضيب معدني يسمى Grounding Rods ذو مقاومة صغيرة ما بين 5 إلى 25 اوم يغرس في الأرض لثمانية أقدام و لهذا فلابد أن يصنع من مواد مقاومة قابلة للصدأ أو التآكل على المدى القصير مثل الحديد المجلفن أو الستانليس ستيل أو النحاس و هذا طبقا للمواصفات الخاصة بالجزء 12.2.2 من المعيار العالمي EIA/TIA 222F
و عندما تكون الهوائيات موضوعة على أبراج مثل أبراج المحمول فإن القضبان الأرضيةGrounding Rods يتم وضعها عند كل أرجل البرج و تكون هذه القضبان متصلة بشكل دائري كما بالشكل

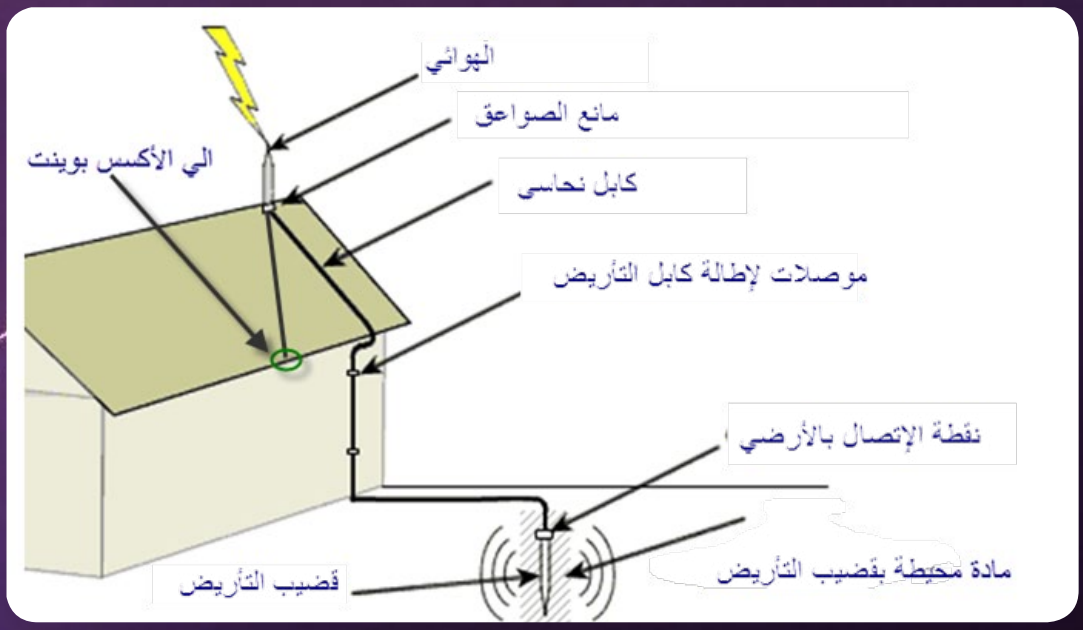
و تقوم سيسكو بإنتاج مانع صواعق (AIR-ACC245LA-R) يستخدم مع أجهزة access points و bridges أو أي جهاز لاسلكي يتم توصيله باستخدام موصلات RP-TNC



يتم تصميم موانع الصواعق لوضعه بين الهوائي و الأكسس بوينت و هذا صالح على طول الكابل المتصل بينهما, أي تستطيع أن تضعه في الشبكة الداخلية أو الخارجية للمنظومة اللاسلكية و تستطيع أيضا أن تربطه بشكل مباشر بالهوائي أو الأكسس بوينت عند توفر موصلات RP-TNC
و كلما كان مانع الصواعق قريب أكثر من الهوائي كلما كان أفضل, حيث أنه من الطبيعي أن يكون هو الحاجز الأول و خط الحماية لكل الأجهزة في الشبكة و المعدات التي ترتبط على خط الهوائي-الأكسس بوينت مثل مكبرات الإشارة Repeater و المجزئات Splitter و المهدئات attenuators
و لابد أن تكون الكابلات الواصلة بين مانع الصواعق و الأكسس بوينت أو الهوائي قصيرة حتى لا تتسبب في فقد كبير في الإشارة



و هذا مخطط كامل لشبكة التأريض تبين كل جزء فيها :



من أهم الأشياء التي لابد أن نعلمها هي أن مانع الصواعق لا يحمي الهوائي نفسه حيث أن الهوائي معرض للتلف تماما إن قام البرق بضربه بشكل مباشر
و أيضا لابد أن تعلم أن مانع الصواعق صالح للاستخدام فقط لمرة واحدة و ذلك عند تعامله مع التيار الناشئ عن طريق البرق, حيث أنه يشبه Fuse و نجاحه في حماية الشبكة يدل على انتهاء مهمته و احتراق مادته الداخلية و لابد من تبديله أو تبديل القطعة التي تلفت فيه إن كان ذلك ممكنا

شهادة شكر وتقدير

تتقدم إدارة موقع

NetworkSet

First Arabic Magazine for Networks

بالشكر والتقدير للمهندس السوري

تميم أحميش

جهوده الكبيرة في مساعدتنا على ترجمة عدد كبير

من المقالات الاحترافية في مجال تقنية المعلومات

مؤسس ومدير موقع NetworkSet

المهندس أيمن النعيمي

2012/1/26



ماهي خاصية IP Service Level Agreement (IP SLA) ؟



يقوم العديد من مهندسي الشبكات بإنشاء شبكة ممتازة وتوفر العديد من الخدمات المتقدمة، لكن إذا حدثت مشكلة ما فإنهم يتيهون ولا يعرفوا من أين يبدؤون وذلك نتيجة للضغط المسلط عليهم من طرف رئيسهم والمستخدمين أو الزبائن، مما يؤدي إلى توترهم وإطالة أمد حل المشكلة، وهذا يكون عادة لغياب تطبيقات لمراقبة أداء الشبكة التي عادة ما تساعدنا على تجنب حدوث المشاكل أو على تحديد مكامن الخلل في الشبكة، في هذا المقال سنحاول التحدث حول وسيلة من وسائل مراقبة أداء الشبكة الموجودة في عالم سيسكو وهي Cisco IOS IP Service Level Agreement (IP SLA) .



Cisco IOS IP Service Level Agreement (IP SLA)هي وسيلة لمراقبة الشبكات و لجمع المعلومات عن أداءها ، تستند على مفهوم توليد (generating) الترافيك في فاصل زمني محدد ، مع إعدادات محددة ، و يتم قياس النتائج المحصل عليها. وهي مبنية على source-responder model، حيث يقوم جهاز واحد (المصدر) بتوليد الترافيك، وإما ينتظر ردا من جهاز آخر (المجيب)) أو يقوم جهاز آخر معد مسبقا بالتقاط الترافيك المرسل ويفعل شيء ما به. هذا النموذج يوفر القدرة الفعلية لتحليل أداء الشبكة مع مرور الوقت، في ظل ظروف محددة، كما يقوم بقياس الأداء، وتجنب انقطاع التيار، وتقييم جودة الخدمة (QoS) ، وتحديد المشاكل والتحقق من مستوى الخدمة، والحد من انقطاع الشبكة.

ميزةIP SLA تسمح بقياس الخصائص التالية في أداء الشبكة:

- (Delay (one way & round trip
- (Jitter (directional
- (Packet loss (directional
- Packet sequencing
- (Path (per hop
- وقت التحميل من الخادم أو الموقع
- الاتصال من خلال وظائف UDP Echo, ICMP Echo, ICMP Path Echo و TCP Connect.
- (Voice-quality metrics (MOS

IP SLA تحقق ما إذا كانت عناصر الشبكة، مثلIP address موجودة في واجهة الروتر أو منفذTCP مفتوح علىHost ما، active و responsive.

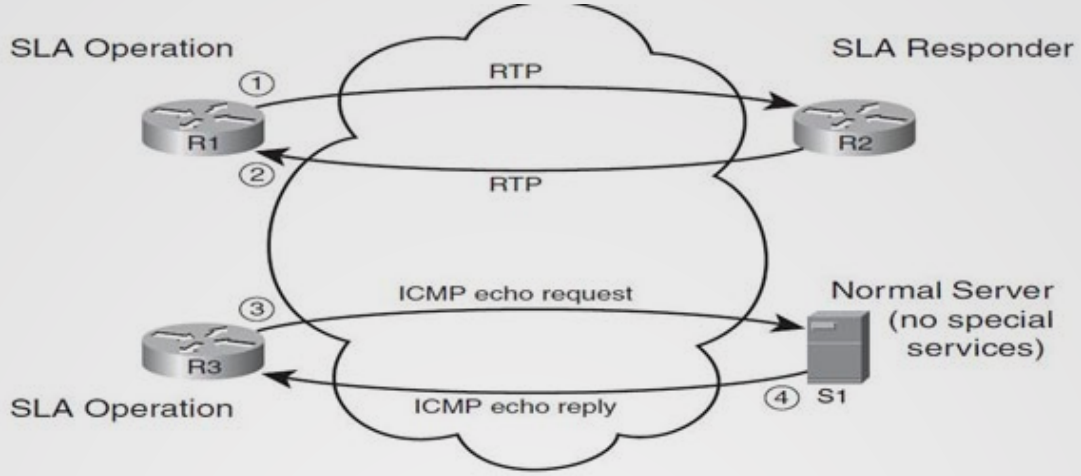
1. كيفية عمل Cisco IOS IP SLAs :

IP SLA تستخدم مفهوم العملية (operation)، كل عملية تحدد نوع الـ Packet التي سوف يولدها الروتر،Source و Destination ip address وغيرها من خصائص الحزمة. تتضمن الإعدادات والوقت التي سوف يرسل فيه الروتر هذه الحزم،وأنواع الإحصائيات التي ينبغي جمعها، وعدد المرات التي يجب ان ترسل فيها الحزم.

على سبيل المثال، يمكن لعملية IP SLA تحديد ما يلي :

- استخدام ICMP echo packets
- قياس end-to-end round trip response (time (ICMP echo
- إرسال الحزم كل 5 دقائق، طول اليوم.

جميع عمليات IP SLA تعتمد على روتر يقوم بإرسال الحزم وبعض الأجهزة الأخرى تقوم بالإيجاب عنها . الشكل أسفله يوضح الفكرة العامة، ويوفر خلفية جيدة لمناقشة بعض القضايا ذات الصلة.



إرسال واستقبال الحزم معIP SLA

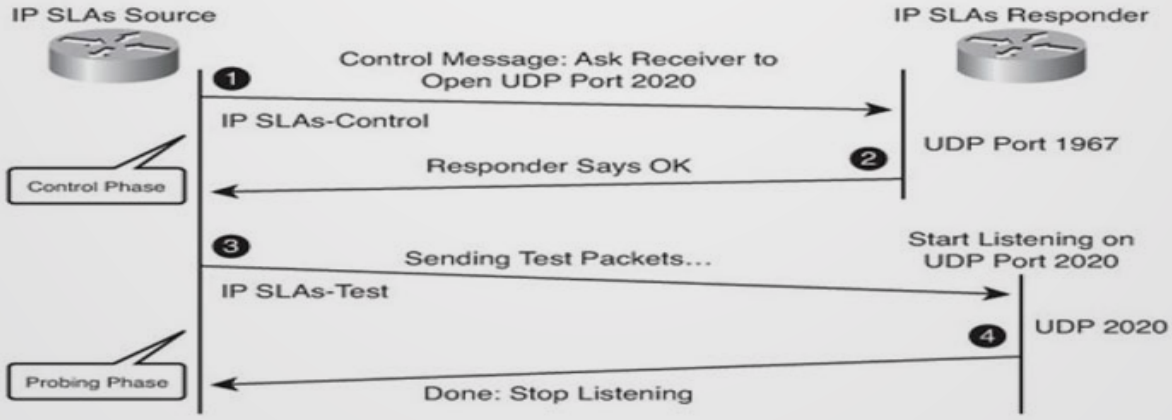
عن طريق عمليةIP SLA يمكن لروتر بإرسال الحزم إلى أي عنوانIP ، سواء إلىhost أو روتر، عند إرسالها إلى host ، كما في الجزء السفلي من الشكل أعلاه، host لا يحتاج إلى أي برنامج خاص أو إعدادات مسبقة ، بدلا من ذلك ، الـ host يعمل كالمعتاد. وهذا يعني أنه إذا كانت عملية IP SLA ترسل الحزم إلى host، يمكن للروتر فقط استخدام أنواع العمليات التي تقوم بإرسال الحزم التي يدركها الـ host. على سبيل المثال، يمكن للروتر استخدام TCP connection، ICMP echo requests requestsأو حتى إرسال HTTP GET requests إلى خادم الويب ، لأن الخادم سيحاول الإجابة عن هذه الطلبات.

يمكن لعمليةIPSLA أيضا أن ترسل الحزم إلى روتر آخر، مما يعطي للـIP SLA مجموعة واسعة من أنواع العمليات المحتملة. إذا كانت العملية سوف ترسل الحزم إلى روتر بعيد سيرد بشكل طبيعي ، مثل ICMP echo requests، في هذه الحالة الروتر لا يحتاج إلى إعداد خاص. مع ذلك، IP SLA تدعم مفهوم IP SLA responder ، كما يلاحظ في الشكل أعلاه، حيث تم إعداد R2 كـ IP SLA responder للإجابة عن الحزم التي لن يجيب عنها عادة، حيث يعطي هذا لمهندس الشبكة وسيلة لرصد عمل الشبكة دون الحاجة لوضع أجهزة في بعض أنحاء الشبكة وذلك لاختبارها فقط .

على سبيل المثال، يمكن لعملية إرسال حزم Real-time Transport Protocol (RTP) ، حزم لديها نفس المحتوى كحزمVOIP ، كما هو مبين في الشكل أعلاه في الخطوة 1. ثم يمكن بعد ذلك لـ R2 بالرد كما لو أن هناك مكالمة صوتية قائمة بين الجهازين، كما هو موضح في الخطوة 2 من الشكل.

2. مثال لاستعمال Cisco IOS IP SLAs مع Responders :

استخدام IP SLA responder يتيح تعزيز مستوى دقة القياس من دون الحاجة لأجهزة أخرى (Thirdparty device) ويمنح إحصائيات إضافية لا تتوفر من خلال بروتوكول ICMP. المصدر يستخدم IP SLAs control protocol للتواصل معResponder قبل إرسال حزم الاختبار. لزيادة أمن رسائل IP SLAs control ، يمكن استخدام MD5 Authentication ما بينSource و Responder. يحدث التسلسل التالي من الخطوات لكل عمليةIPSLA تتطلب الرد منResponder ، كما هو موضح في الشكل أدناه :





. في بداية المرحلة الـ control يرسل source رسالة Control تتكون من معلومات عملية IP SLA المعدة إلى IP SLAs control port UDP 1967 في Responder router ، رسالة الـ control تتضمن البروتوكول ، رقم المنفذ ، ومدة العملية. مبين في الرسم أعلاه ، يتم استخدام المنفذ UDP 2020 لاختبار حزم IPSLA .

إذا تم إعداد MD5 authentication ، يتم إرسال MD5 checksum مع رسالة الـ control ، ويتحقق responder من MD5 checksum . إذا فشلت عملية authentication يقوم بإرجاع رسالة « authentication failure».

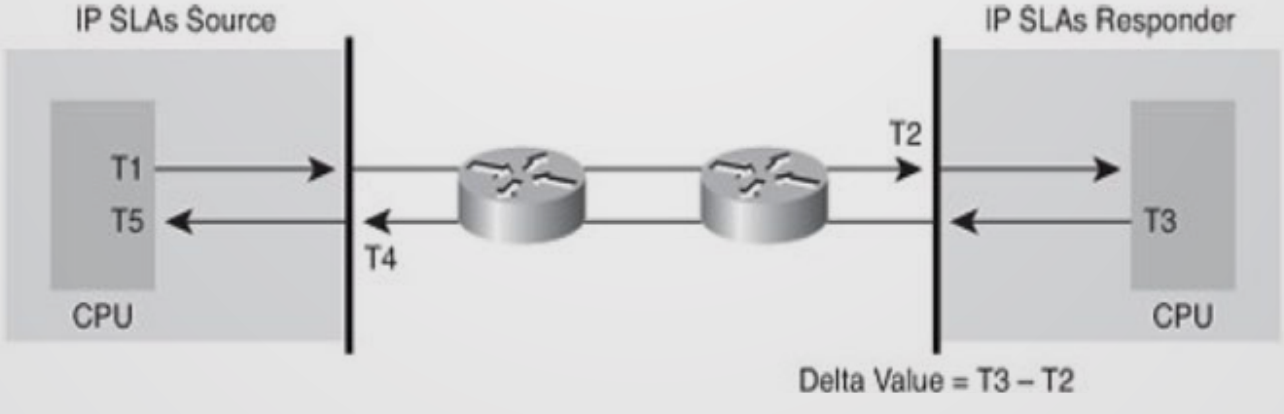
2. إذا ما قام Responder بعمل process لرسالة ال control ، فإنه يرسل رسالة « OK» إلى المصدر ويستمع على المنفذ المحدد في رسالة الcontrol لمدة محددة. أما إذا كان لا يستطيع عمل process لرسالة الcontrol ،فإنها يرجع رسالة error إلى المصدر.Responder قادر على الاجابة على عمليات IP SLA متعددة تحاول الاتصال إلى نفس رقم المنفذ.

3. إذا تم إرجاع رسالة «OK» ، تنتقل عملية IP SLA إلى مرحلة probing حيث يقوم المصدر بإرسال عدة حزم اختبار إلى responder لحساب وقت الإجابة (Time responses) .يتم إرسال رسائل الاختبار على منفذ 2020.

4. يقبل Responder حزم الاختبار ويجيب عليها بناء على نوع العملية، قد يقوم بإضافة "in" time stamp و "out" time stam في حزمة الإجابة، وذلك من أجل مساعدة CPU على حساب وقت unidirectional packet Latency، loss ، وJitter . هذه الطوابع الزمنية (Time stamp) تساعد مصدر IPSLA على إجراء تقييم دقيق لاتجاه واحد من delay، ووقت الـ processing في responder. يقوم responder بتعطيل المنفذ المحدد من قبل المصدر بعد أن يجيب على الحزم أو عند انتهاء الوقت المحدد.

3. Cisco IOS IP SLAs with Responder : Time Stamps

يوضح الشكل أسفله استخدام طوابع الوقت لحساب الوقت ذهابا وإيابا (round-trip) في عملية IP SLA تستعمل Responder . مصدرالـ IP SLA يستخدم أربع طوابع زمنية لحساب وقت (round-trip time)RTT) .



مصدر الـ IP SLA يرسل حزم الاختبار في اللحظةT1 بسبب بعض العمليات الأخرى ذات الأولوية العالية, قد يستغرق الروتر عشرات الميلي ثواني لعملprocess للحزم الواردة، على سبيل المثال، قد يكون الرد على حزمة الاختبار موجود في طابور الانتظار لتتم معالجته، لحساب هذا التأخير(delay)، يضعresponder كلا من لحظة الاستلام (T2) و لحظة الإرسال (T3) في حزمة الإجابة, لهذا فإن طوابع الوقت دقيقة إلى حد sub-milliseconds.
مصدر الـIP SLA يطرح T2منT1 لتحديد قيمة دلتا، الوقت المستغرق لمعالجة حزمة الاختبار على مستوى Responder . يتم تطبيق نفس المبدأ في مصدر IP SLA بطرح T4 من T5 لتحديد قيمةRTT . لحساب هذا التأخير ، يجب أن يتزامن المصدر والمجيب من نفس مصدر الساعة، وبالتالي، لا بد من إعداد بروتوكول Network Time Protocol (NTP).

4. إعداد Cisco IOS IP SLAs:

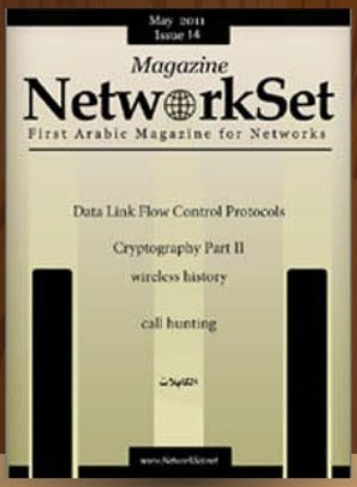
الخطوات العامة لإعداد ICMP-based IP SLA هي كما يلي :

- الخطوة 1 : إنشاء عمليةIP SLA ، وتعيين عدد صحيح للعملية، وذلك باستخدام أمر-ip sla sla-ops number .
- الخطوة 2 : تحديد نوع العملية والخصائص لهذا النوع من العملية، بالنسبة لـ ICMP echo، يمكنك تحديد عنوان IP للوجهة أو اسم الوجهة ، واختياريا، عنوانIP للمصدر أو اسم الوجهة، وذلك باستخدام أمرicmp-echo {destination-ipaddress| destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name]

- الخطوة 3 : اختياريا يمكن تحديدfrequency العملية أي عدد الحزم المرسلة في الثانية، وذلك باستخدام أمر frequency seconds .
- الخطوة 4 : إعداد وقت تشغيلIP SLA ،وذلك باستخدام أمر. ip sla schedule sla-ops-number [life {forever | seconds}] [start-time {hh:mm[:ss] [month day | day month] |pending | now | after [hh:mm:ss]} [ageout seconds] [recurring]

بهذا نكون قد انتهينا من شرح هذه التقنية التي يمكنها مساعدتنا في اختبار ومراقبة العديد من الأشياء في الشبكة. أتمنى أن أكون قد وفقت في الشرح وأضفت شيء للمحتوى العربي كما أتمنى أن ألقاكم في موضوع قريب إن شاء الله.حفظكم الله ورعاكم.

Network Set Magazine Gallery



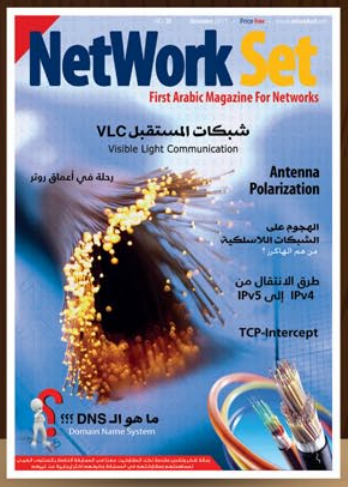




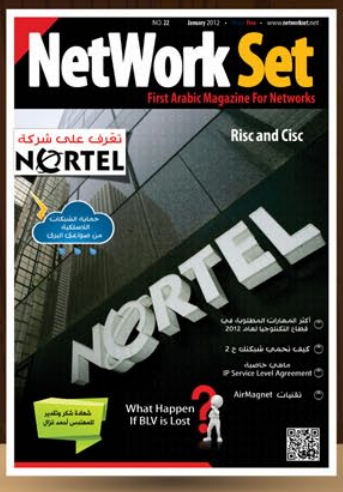












تقنيات AirMagnet

لاشك بأنك للمرة الأولى تسمع عن تقنيات AirMagnet . ولاشك أنك متشوق الأن لمعرفة ماذا تقدم هذه التقنيات ؟

تقنيات AirMagnet مقدمة من شركة Fluke الألمانية, وهي من أقوى الشركات المتخصصة في تصنيع أدوات فحص مبتكرة توفر خدمات احترافية لمهندسي الشبكات وغيرها من الأدوات التي تتعلق بالكهرباء والمجالات الأخرى . إلّا أننا في هذا المقال نسلط الضوء على أحد تقنياتها وهي تقنية Airmagnet Enterprise, وذلك بعد أن تحدثنا في عدد سابق عن عدة أدوات لفحص الشبكات و المقدمة من شركة Fluke .

ماذا تقدم تقنيات AirMagnet ؟؟

صممت تقنيات AirMagent لدعم تقنية الـ Wi-Fi المنتشرة في الشركات و المشاريع الضخمة, حيث تتخصص هذه التقنيات في عدة مجلات منها التحليل والتصميم والحماية وضبط الأداء في الشبكات المبنية على الأجهزة اللاسلكية والتي تندرج تحت المعيار IEEE 802.11 . وسنحدثكم اليوم عن أحد تقنيات AirMagnet وهي تقنية AirMagnet Enterprise .



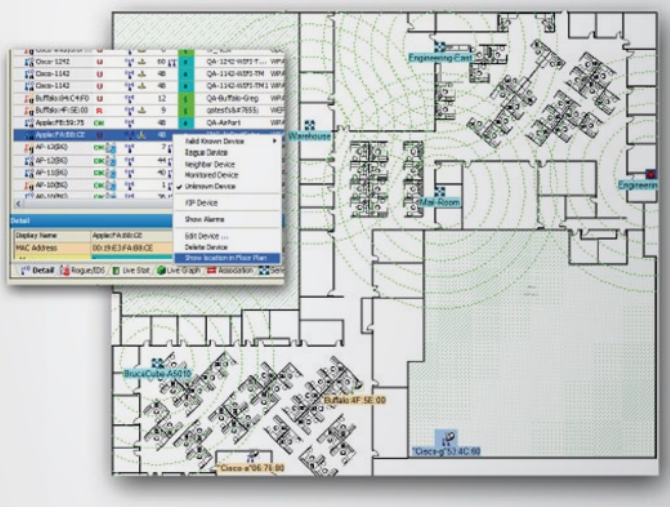
تقنية AirMagnet Enterprise :



هذه التقنية هي من أحد أقوى التقنيات المستخدمة في إدارة الشبكات اللاسلكية الضخمة, وتتكون هذه التقنية من هاردوير يرتبط بسوفت وير منصب على سيرفر, حيث تقدم هذه التقنية لمهندسي الشبكات ميزات غريبة وعجيبة بشكل مفصل ودقيق عن الشبكة اللاسلكية الضخمة التي يقومون بإدارتها . حيث تسهل عليهم العمل وتجعله أكثر متعة وتزيل التعقيد عنهم لأن فحص الشبكات اللاسلكية الضخمة التي تحتوي على مئات من نقاط البث وآلاف المستخدمين ليس بالأمر السهل.

تقدم هذه التقنية أمان عالي جداً في الشبكات اللاسلكية حيث تستطيع كشف Rogue Access Points أي نقاط البث التي تم توصيلها بطريقة غير شرعية ودون علم مدارء الشبكة . وعند كشف أي من هذه AP التي تم توصيلها بطريقة غير شريعة, تقوم هذه التقنية مباشرةً بتنبيه مدراء الشبكات وإصدار صوت إنذار, وبعد ذلك يرجع

المهندسين للنظام وفتح برنامج التحليل والإدارة الذي سيكشف لهم موقع نقطة البث وعلى أي منفذ موصلة وعنوانها والـ SSID الخاص بها والحماية المستخدمة فيها والمستخدمين المتصلين بها كما هو موضح في الصورة التالية :



كذلك تتيح هذه التقنية إرسال رسالة عبر البريد الإلكتروني في حالة حدوث خطر, بحيث يستطيع كل مهندس في حال لم يكن متواجد في العمل أن يضع بريده الإلكتروني في البرنامج ليتلقى رسالة في حالة حدوث خطر ما على الشبكة . وأيضا يمكن تفعيل بروتوكول SNMP الخاص بإرسال تقارير لمدراء الشبكة, كما يمكنك أيضاً تفعيل خاصية Print التي تقوم مباشرةً بطباعة تقرير عن المشكلة الحاصلة .

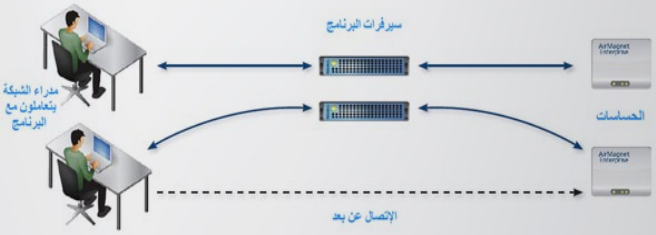


كذلك تتميز هذه التقنية بتحديد Policies أو سياسات ربط واستخدام نقاط البث ، حيث يستطيع مدراء الشبكة تحديد الـ SSID أو اسم الشبكات وأنواع الحمايات المستخدمة فيها والـ Channel أو قنوات البث المستخدمة وكذلك التردد أو الـ Frequency المستخدم . فعند توصيل أي Access Point بالشبكة يستخدم إعدادت لا تتوافق مع ما حدده المدراء ، فإن النظام سيقوم بحجب المنفذ الموصل بذلك الـ Access Point أو يقوم بإعلام المدراء مباشرةً عن تفاصيل وموقع ذلك الـ Access Point .

والجدير بالذكر أن هذه التقنية تحتوي على IPS أو Intrusion Prevention System منفصل ، وكما تعلم أن هذا الجهاز يستخدم في التصدي ومنع الهجمات على الشبكة , وكذلك تتضمن هذه التقنية بما يسمى Sensor أو الحساس كما هو في الصورة التالية :



حيث يقوم هذا الحساس بالكشف عن الأجهزة اللاسلكية التي لا تندرج تحت المعيار 802.11 مثل تقنية البلوتوث وكاميرات المراقبة اللاسلكية التي تم توصيلها مع الشبكة بطريقة غير شرعية ودون علم المدراء . يمكنك نشر أكثر من 1000 حساس في شبكتك لتنبهك بأي خطر أو تعارض في الترددات يحدث في أي موقع من الشبكة . وهذه صورة توضح استخدام هذه التقنية :



وتوفر هذه التقنية مسح دقيق وبشكل دوري عن صد الهجمات التي قد تحدث . فتقوم هذه التقنية بعمل مسح لكل الأجهزة اللاسلكية وتسجيل أي هجوم يحدث وكتابة وصف عنه في قاعدة بيانات خاصة وتسجل الـ Signature الخاص به إذا كان هناك أحد الفيروسات أو ملفات التجسس, بحيث لو حدث مرة أخرى تستطيع هذه التقنية مباشرةً كشفه وذلك من خلال الـ Signature المسجل في قاعدة البينات . كذلك تمتلك هذه التقنية القدرة على التقليل من DoS Attack و Dos Attack 802.11n والأدوات المتطورة مثل أدوات Metaspolit وكشف Man-in-the-Middle .

كما أن هنالك تحديثات مستمرة لهذه التقنية وذلك لصد الهجمات الجديدة . وهنالك أيضاً سجلات في هذه التقنية تسجل تحركات المهاجمين وكم هي كمية البيانات التي استهلكوها أثناء الهجوم, ومن المميزات الرائعة أيضاً ، هي أن هذه التقنية تقوم بتسجيل الأحداث قبل تأثيرها على المستخدمين وتنبه المدراء مباشرةً .

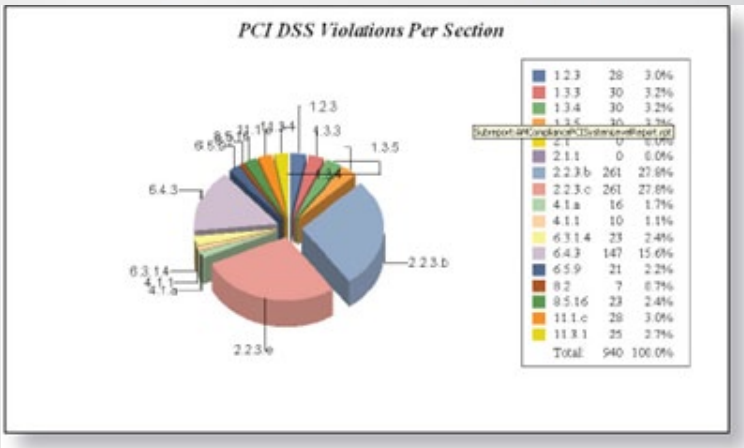
أما فيما يتعلق بالـ Troubleshooting و Optimization ، فإن هذه التقنية تقدم الكثير والمفيد .

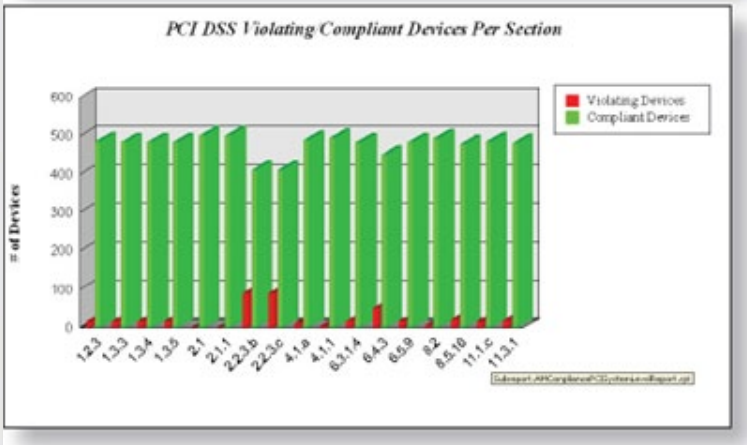


فتزودنا هذه التقنية بتقرير عن كافة المستلزمات التي نحتاجها من أجل أن تكون الشبكة اللاسلكية قادرة على العمل على مدار الساعة وأن تكون جميع الخدمات متاحة في كل الأوقات . كما أنها تزود مدراء الشبكات عن المشاكل المتعلقة بإعدادات الأجهزة اللاسلكية وكذلك المشاكل المتعلقة بعملية انتشار الإشارة أثنا التجوال, بحيث يستطيع المهندس إيجاد المشكلة بسهولة ويسر وكشف المناطق التي تنعدم فيها الإشارة, وكذلك المناطق التي يحدث فيها تعارض وتشويش في الإشارة, حيث تكتشف الحساسات المناطق التي منع فيها استخدام Channel معين وذلك بالرجوع للـ Policy التي أعدها مدراء الشبكة فتنبههم في حال استخدام Channel أو تردد مخالف في منطقة معينة . ومن الميزات الذكية في هذه التقنية أيضاً ، هي أنها قادرة على تزويد المهندسين بتقرير عن الأجهزة التي تستخدم Mode N في البث . فتخبرهم بحالة الـ Bandwidth المستهلك وكيف يمكن زيادته



وتحسين الأداء بشكل أفضل, لأنه و كما تعلم أن Mode N يستخدم سرعة عالية لنقل البينات تصل إلى 300Mbps والتي يمكن أن نستغلها في نقل الفيديو ولعب ألعاب الفيديو على الشبكة .





وخلاصة لهذا المقال ، إننا ننصح كل مهندس شبكات لاسلكية أن يتطلع لهذه التقنيات وأن يتعمق في مجال تحليل الشبكات اللاسلكية أو Wireless Networks Analysis وبهذا يمكن للمهندس أن يحترف في الشبكات اللاسلكية وأن يصبح خبيرا في حل المشاكل التي تتعلق بها.



أهم عشرة أشياء يجب أن تعلّمها للمستخدمين

في عالم التكنولوجيا والشبكات لا يحتاج المستخدمين العاديين معرفة كاملة عن كيفية عمل أجهزة الكمبيوتر أو كيفية تكوين الشبكات وكيفية عملها , ولكن من المهم تعليمهم القليل من الفنيّات الخاصة بالأجهزة من هنا و هناك أي على الأقل فهم الحد الأدنى من تكنولوجيا المعلومات .وسوف أطرح في هذا المقال قائمة تضم بعض الأساسيات التي يجب على كل مستخدم تعلمها وهو يشمل بعض الاجراءات والنصائح التي يجب التقيد بها لتوفير الوقت والأمان ورفع الفعالية أكثر .

قم بإعادة التشغيل قبل أن تتصل بمكتب الدعم .

أعتبر القاعدة الأولى والأهم التي يجب أن نُعلّمها للمستخدمين عند ظهور أي مشكلة لديهم هي إعادة تشغيل الجهاز قبل أن تقوم بأي اتصال مع مكتب الدعم, وخصوصا أن تجاربنا العملية مع عالم حل المشاكل يقول لنا (لا دليل علمي) أن إعادة إقلاع المشاكل يساعد في حل مشاكل كثيرة , ولو لم تحل المشكلة عندها فقط يتصل مع مكتب المساعدة والدعم .

طريقة الإبلاغ عن المشكلة

النقطة الثانية التي يجب أن تحرص على تعليمها للمستخدمين هو كيفية تجهيز التقرير الخاص بالمشكلة وكيفية طرحه على مكتب الدعم , فالمستخدمين يجب أن يعلموا ماهي المعلومات التي يحتاجها مكتب الدعم من المستخدمين أو من الأجهزة التي تحوي مشاكل مثل: رسالة الخطأ , البرامج التي تعمل , ماذا كنت تفعل عندما حدثت المشكلة , متى تزيد المشكلة أو تتفاقم , هذه الأسئلة التي تسألها مكاتب المساعدة للمستخدمين ويجب على المستخدمين أن يتعلموا هذه الأسئلة ويكونوا على دراية كاملة بكيفية الإجابة عنها .

إبقاء كلمات السر في مكان آمن

هناك الكثير ممن يهملوا حفظ كلمة المرور الخاصة بأجهزتهم بكتابتها في أماكن غير آمنة أو سرية , فلقد شاهدت أناس تكتب كلمة السر على الحائط الموجود على جانبها وهناك من يكتبه على ورقة صغيرة ويلصق الورقة على حرف الشاشة أو على جانب الـ Case الخاص بالكمبيوتر, بل وهناك من يكتبه على يده أو في شاشة السكرين سيرفر وبخط واضح ومفهوم , كل هذه الأمور يجب التحذير منها ويجب تعليمها للمستخدمين وتوضيح المخاطر التي تترتب على معرفة كلمة السر الخاصة بالدخول إلى جهازه .



إنشاء كلمة مرور آمنة

يجب دائما استخدام أسلوب التثقيف مع المستخدمين بإنشاء كلمات المرور أي إعطائهم فن تشكيل كلمة المرور فهي التي سوف تضمن لنا سلامة النظام من المتسللين ويجب دائما تجنب أسماء أفراد الأسرة، والأرقام التسلسلية مثل 123456 والكلمات والعبارات الواضحة, ودائما ينصح بكتابة أرقام عشوائية وعلامات الترقيم .

ممارسة الحوسبة الآمنة أثناء السفر.

الكثير من المستخدمين عادة ما يأخذون الأجهزة المحمولة أو الأجهزة اللوحية إلى خارج العمل, لذلك وجدت أن النقطة الخامسة التي يجب أن تعلمها لمستخدميك هي كيفية حماية أجهزتهم المحمولة , ومن أهم الملاحظات التي يجب التحذير منها هي عدم وضع أي كلمات سر أو مفاتيح معينة للدخول بالإضافة إلى المعلومات الحساسة والتي تمس بأمن الشركة أو تمس أحد من عملائها, ولو في حال كان لابد من وجود بعض المعلومات على الجهاز فالأفضل الاحتفاظ بها مشفرة أو على فلاش خارجي , وأخيرا عدم ترك المستخدم للجهاز بعيدا عن ناظريه.



منع فقدان البيانات

يحتاج المستخدمين لمعرفة أن النسخة الاحتياطية هي الحل الأوحد لمنع ضياع البيانات إذا حذفت في الخطأ, لذا يجب تعويد المستخدمين على أوقات معينة للقيام بعملية النسخ الاحتياطية , وتوضيح ماهي الملفات التي يجب عمل نسخ احتياطية منها وطبعا هذا الأمر لاينطبق على كل أنواع المستخدمين وهي تنحصر مع المستخدمين الذين يحملون أجهزتهم معهم إلى الخارج , لأن تأمين وحماية الملفات الموجودة داخليا هي مهمتك وليست مهمة المتسخدمين, لكن الإشارة هنا إلى النوع الثاني من المستخدمين .

توضيح سياسات الاستخدام

معظم الشركات في عالمنا تطبق سياسات صارمة ونظام فعّال في ساعات العمل, وهذا يكون لصالح الشركة وأداء عملها وهو شيء ايجابي للحفاض على سمعتها والحفاظ على البنية التحتية لتكنولوجيا المعلومات, ودائما مثل هذه الشركات تقوم بمتابعة ومراقبة المستخدمين وهذا طبعا لا يمثل لعب دور الشرطة بل شرط ضروري لاستمرارية نظام العمل في الشركة, لذلك وجدت أن توضيح السياسات الخاصة بالشركة شيء ضروري, ويجب توضيحه لكل المستخدمين حتى نضع النقاط على الحروف وحتى يعلم ماهو المسموح؟ وماهو الممنوع استخدامه؟ وماهي صلاحياتهم؟ .

الحذر في إرسال رسائل البريد الإلكتروني

كم مرة ذكر لك أحدهم أنه قد قام بإرسال رسالة إلكترونية إلى شخص معين بالخطأ؟ وكم منهم أرسل رسائل شخصية جدا أو سرية للغاية؟. لذا فالنقطة الثامنة سوف تكون حول موضوع التأكد من اسم الشخص المرسل إليه وتوضيح مضار هذا الأمر ببعض الأمثلة الحقيقية التي نسمع بها, لذلك إنصح مستخدميك بالتأكيد أكثر من مرة قبل الضغط على زر الإرسال .

حماية ضد الفيروسات، والتصيد، والبرمجيات الخبيثة، وغيرها من الأخطار

المعاناة الكبرى التي يعاني منها المسؤول المختص بحماية الشبكة هي الحفاظ على شبكتهم من المتطفلين الذين يسعون إلى تخريبها وهي طبعا جزء كبير من وظيفته, لكن هناك جزء هام أيضا يعتمد على المستخدم نفسه, لذلك نحن مضطرون للاعتماد على اليقظة العامة للمستخدم . مثل توضيح خطورة فتح الرسائل المجهولة المصدر وتوضيح خطورة الهندسة الاجتماعية ومواضيع التصيد والاحتيال الإلكتروني وكذلك التنبيه إلى ضرورة التأكد من وجود آخر التحديثات المتعلقة بأنظمة الحماية ومضاد الفايروسات بالإضافة إلى تحديثات الويندوز .


Magazine
NetworkSet
www.networkset.net